Aplicación Citrix Workspace

Contents

Aplicación Citrix Workspace 3

Extensiones web de Citrix Workspace 7

App Protection 9

Requisitos del sistema y compatibilidad 18

Funciones de App Protection 22

Configurar App Protection 30

Configurar la protección contra el registro de tecleo y capturas de pantalla 38

Configurar la antiinyección de DLL 46

Configurar la detección de manipulación de directivas 52

Configurar la verificación de postura de App Protection 53

Bloquear inicio de doble salto 61

Configurar Lista de permitidos para capturas de pantalla 61

Configurar Lista de exclusión de procesos 66

Configurar Lista de exclusión de controladores de filtro USB 69

Solucionar problemas técnicos 76

Solución de problemas genéricos 78

Solucionar problemas técnicos de detección de manipulación de directivas 82

Solución de problemas técnicos de la verificación de la postura de App Protection 85

Recopilación de registros 88

Contextual App Protection para Workspace 90

Requisitos previos 91

Caso 1 91

Caso 2 96

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

Caso 3 104

Caso 4 106

Contextual App Protection para StoreFront 108

Requisitos previos 110

Caso 1 110

Caso 2 114

Caso 3 116

Caso 4 117

Caso 5 120

Compatibilidad de App Protection con el inicio híbrido a través de Workspace 120

Compatibilidad de App Protection con el inicio híbrido a través de StoreFront 125

Calendario de publicación de versiones de la aplicación Citrix Workspace 133

Tabla de funciones de la aplicación Citrix Workspace 139

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

Aplicación Citrix Workspace

April 25, 2024

Acerca de la aplicación Citrix Workspace

La aplicación Citrix Workspace proporciona un acceso instantáneo, seguro y directo a todos los recursos que los usuarios finales necesitan para seguir siendo productivos. La aplicación Citrix Workspace incluye el acceso a escritorios virtuales, aplicaciones virtuales, aplicaciones web y SaaS, y funciones como la navegación integrada y Single Sign-On (desde cualquier lugar y desde cualquier dispositivo).

La aplicación Citrix Workspace es una aplicación cliente que se puede implementar en todos los dispositivos, tanto en entornos locales como en la nube. Se basa en las prestaciones de lo que antes se conocía como Citrix Receiver e incluye tecnologías cliente de Citrix, como HDX, los plug-ins de Citrix Gateway y Secure Private Access.

La aplicación cliente está optimizada para ejecutarse en todos los sistemas operativos cliente, como Windows, macOS, Linux, iOS y Android. También se puede acceder a ella a través de un explorador web. Para obtener más información sobre los exploradores web compatibles, consulte Workspace Browser Compatibility.

La aplicación Citrix Workspace, que emplea el protocolo de Citrix y HDX (experiencia de alta definición), entrega sesiones de escritorios y aplicaciones virtuales de alto rendimiento. Se ha mejorado para ofrecer una experiencia segura en inicios de sesión y en la navegación por Internet, una administración sencilla de sus aplicaciones y escritorios, funciones de búsqueda avanzada y más.

> **Nota:**
>
> La interfaz de usuario de la aplicación puede variar en función de la implementación de los recursos; es decir, en la nube (al aprovechar la plataforma Workspace) o de forma local (al aprovechar la plataforma StoreFront).

Para obtener información sobre las funciones disponibles en la aplicación Citrix Workspace, consulte Tabla de funciones de la aplicación Citrix Workspace.

Para obtener información acerca de las diferencias entre las versiones actuales (Current Release) y LTSR, consulte Lifecycle Milestones for Citrix Workspace app.

La aplicación Citrix Workspace está disponible para los siguientes sistemas operativos:

- Aplicación Citrix Workspace para Android
- Aplicación Citrix Workspace para ChromeOS

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

- Aplicación Citrix Workspace para HTML5
- Aplicación Citrix Workspace para iOS
- Aplicación Citrix Workspace para Linux
- Aplicación Citrix Workspace para Mac
- Aplicación Citrix Workspace para Windows
- Aplicación Citrix Workspace para la Tienda Windows

> **Muy importante**
>
> **Datos recopilados para las actualizaciones de la aplicación Citrix Workspace:**
>
> Con relación a los dispositivos conectados a Internet, la aplicación Citrix Workspace podría, sin previo aviso, comprobar si hay actualizaciones disponibles para su descarga e instalación en el dispositivo y notificar al usuario su disponibilidad. Cuando esto sucede, solo se transmite información no personal, excepto en la medida en que las direcciones IP puedan considerarse información identificable de personas en algunas jurisdicciones.

Configurar la aplicación Citrix Workspace mediante Global App Configuration Service

Global App Configuration Service proporciona una interfaz centralizada en la que configurar los parámetros de la aplicación Citrix Workspace para los usuarios finales. Puede configurar los parámetros de almacenes locales y de la nube desde una única interfaz. Estos parámetros se aplican tanto a dispositivos administrados como a dispositivos no administrados (BYOD). Para obtener más información, consulte Global App Configuration Service.

Idiomas disponibles

Las aplicaciones Citrix Workspace están adaptadas para su uso en idiomas distintos del inglés. En esta sección se indican los idiomas disponibles en la versión más reciente de las aplicaciones Citrix Workspace.

En esta tabla se indican los idiomas disponibles en la aplicación Citrix Workspace en varios sistemas operativos o plataformas. Un símbolo ☑ indica que la aplicación está disponible en ese idioma concreto.

Idioma	Android	ChromeOS	HTML5	iOS	Linux	macOS	Windows	Tienda Windows
Inglés	☑	☑	☑	☑	☑	☑	☑	☑

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

Idioma	Android	ChromeOS	HTML5	iOS	Linux	macOS	Windows	Tienda Windows
Danés	☑			☑				
Neerlandés	☑	☑	☑	☑	☑	☑	☑	☑
Francés	☑	☑	☑	☑	☑	☑	☑	☑
Alemán	☑	☑	☑	☑	☑	☑	☑	☑
Italiano	☑	☑	☑	☑	☑	☑	☑	☑
Japonés	☑	☑	☑	☑	☑	☑	☑	☑
Coreano	☑	☑	☑	☑	☑		☑	☑
Portugués (Brasil)	☑	☑	☑	☑	☑	☑	☑	☑
Ruso		☑	☑		☑		☑	☑
Chino simplificado	☑	☑	☑	☑	☑	☑	☑	☑
Español	☑	☑	☑	☑	☑	☑	☑	☑
Sueco	☑			☑				
Chino tradicional		☑	☑				☑	☑

Marca de función

En este artículo se describe la administración de marcas de función y las diversas aplicaciones de Citrix Workspace que permiten usarlas.

Administrar marcas de función

Si se produce un problema con la aplicación Citrix Workspace en producción, podemos inhabilitar de manera dinámica una función afectada en la aplicación Citrix Workspace aunque dicha función ya se haya publicado. Para ello, se utilizan marcas de función y un servicio externo denominado LaunchDarkly. No es necesario que realice ninguna configuración para permitir el tráfico a LaunchDarkly, salvo si tiene un firewall o proxy bloqueando el tráfico saliente. En ese caso, puede habilitar el tráfico a LaunchDarkly a través de direcciones URL o direcciones IP específicas, según sus requisitos de

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

directiva.

En esta tabla se indican las distintas aplicaciones que permiten usar marcas de función y las versiones publicadas en las que se comenzaron a usar marcas de función en estas aplicaciones.

Aplicación	Marcas de función disponibles	Versión	Documentación
Aplicación Citrix Workspace para Android	Sí	10.7.5	Administración de marcas de función para la aplicación Citrix Workspace para Android
Aplicación Citrix Workspace para ChromeOS	Sí	1908	Administración de marcas de función para la aplicación Citrix Workspace para ChromeOS
Aplicación Citrix Workspace para HTML5	Sí	1908	Administración de marcas de función para la aplicación Citrix Workspace para HTML5
Aplicación Citrix Workspace para iOS	Sí	10.4.10	Administración de marcas de función para la aplicación Citrix Workspace para iOS
Aplicación Citrix Workspace para Linux	Sí	2109	Administración de marcas de función para la aplicación Citrix Workspace para Linux
Aplicación Citrix Workspace para Mac	Sí	2010	Administración de marcas de función para la aplicación Citrix Workspace para Mac

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

Aplicación	Marcas de función disponibles	Versión	Documentación
Aplicación Citrix Workspace para Windows	Sí	2012	Administración de marcas de función para la aplicación Citrix Workspace para Windows

Importante actualización sobre Citrix Receiver

Desde agosto de 2018, la aplicación Citrix Workspace sustituye a Citrix Receiver. Aunque aún podrá descargar versiones anteriores de Citrix Receiver, se publican nuevas funciones y mejoras para la aplicación Citrix Workspace.

La aplicación Citrix Workspace es un nuevo cliente de Citrix que funciona de manera similar a Citrix Receiver y es totalmente compatible con la infraestructura de Citrix de su organización. La aplicación Citrix Workspace proporciona todas las prestaciones de Citrix Receiver y las nuevas prestaciones basadas en la implementación de Citrix de su organización.

La aplicación Citrix Workspace se basa en la tecnología de Citrix Receiver y es totalmente retrocompatible con todos los servicios de Citrix.

Para obtener más información, consulte la página de preguntas frecuentes sobre la aplicación Workspace.

Extensiones web de Citrix Workspace

April 25, 2024

Con la extensión web de Citrix Workspace, puede iniciar las aplicaciones de su espacio de trabajo donde quiera sin necesidad de un archivo `.ica`, lo que vuelve su experiencia más segura y fiable. Al abrir las aplicaciones con la extensión para exploradores web, todas las aplicaciones y escritorios se mantienen en una sola ubicación, lo que le permite realizar un seguimiento sencillo de su trabajo y mantener el escritorio limpio. La extensión web de Citrix Workspace también ofrece la ventaja de App Protection contra capturas de pantalla y la continuidad del servicio integrada.

Instalar las extensiones web de Citrix Workspace

Para instalar la extensión web de Citrix Workspace, siga estos pasos:

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

1. Vaya a la tienda web de su explorador web preferido:
   - Chrome Web Store
   - Complementos de Microsoft Edge
   - App Store para Mac
2. Agregue y confirme la instalación de la extensión web de Citrix Workspace a través de la tienda de aplicaciones de su explorador web preferido.
3. Si fuera necesario, confirme el mensaje emergente que pregunta si quiere agregar la extensión web.
4. (Opcional) Seleccione el icono de la pieza del rompecabezas de la parte superior derecha del explorador web para anclar la extensión y acceder al explorador web fácilmente.
5. Seleccione **Agregar extensión**.
6. Seleccione el icono de la chincheta para anclar la extensión.

La extensión web de Citrix Workspace se habrá instalado.

Para obtener información adicional sobre la extensión web de Citrix Workspace, consulte el blog sobre la extensión web de Citrix Workspace.

Abrir aplicaciones SaaS en su instancia de Citrix Workspace

Si la extensión web de Citrix Workspace aún no está habilitada en su instancia de Workspace, siga estos pasos:

1. Seleccione el perfil de su cuenta en la ventana de Workspace.
2. Seleccione **Avanzado** en el menú del perfil.
3. Seleccione **Usar explorador web** en la ventana **Preferencias de inicio de aplicaciones y escritorios**.
4. Confirme **Abrir Citrix Workspace Launcher** en la ventana emergente.

Ahora, sus aplicaciones SaaS se abrirán en la ventana de la aplicación Citrix Workspace.

Tabla de funciones de la aplicación Citrix Workspace

La aplicación Citrix Workspace proporciona una gama de funciones distribuidas en diferentes plataformas o sistemas operativos. Con esta tabla de funciones, podrá comprender claramente la disponibilidad de las funciones en las diferentes plataformas.

Cualquier equipo con un explorador web compatible y una conexión a Internet puede acceder a la extensión web de Citrix Workspace. Para usar todas las características y funciones de la extensión web de Citrix Workspace, se admiten estos tipos de exploradores web:

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

Nombre del explorador web	Versión
Google Chrome	Versión más reciente
Microsoft Edge	Versión más reciente
Apple Safari	Versión más reciente

App Protection

March 11, 2024

App Protection es una función de la aplicación Citrix Workspace que proporciona una seguridad mejorada cuando se utilizan recursos publicados de Citrix Virtual Apps and Desktops. App Protection está disponible en las implementaciones locales de Citrix Virtual Apps and Desktops y Citrix DaaS (antes denominado Citrix Virtual Apps and Desktops Service) con StoreFront y Workspace. Esto significa que App Protection se admite en todos los entornos de nube, locales e híbridos. App Protection también está disponible al conectarse a StoreFront o Workspace a través de ADC Gateway.

Dos directivas proporcionan funciones contra el registro de tecleo y las capturas de pantalla en una sesión de Citrix HDX. Las directivas, junto con la aplicación Citrix Workspace 2203.1 LTSR o versiones posteriores para Windows, Citrix Workspace 2001 o versiones posteriores para Mac o Citrix Workspace 2108 o versiones posteriores para Linux pueden ayudar a proteger los datos de registradores de pulsaciones de teclas y capturadores de pantalla.

Al habilitar la protección contra la captura de tecleo:

- Un registrador ve pulsaciones de teclas cifradas.
- Esta función solo está activa cuando hay una ventana protegida enfocada.

Cuando la función contra las capturas de pantalla está activada:

- En el SO Windows y macOS, al capturar una pantalla, solo queda vacío el contenido de la ventana protegida. Esta función está activa cuando una ventana protegida no está minimizada. En el SO Linux, toda la captura aparece vacía. Esta función está activa tanto si una ventana protegida está minimizada como si no.
- Cuando se usa el botón de **impresión de pantalla** en el sistema operativo Windows para tomar capturas de pantalla, los datos no se copian en el portapapeles. Para tomar capturas de pantalla con el botón de **impresión de pantalla**, minimice las aplicaciones protegidas.

Las directivas se configuran mediante PowerShell y Web Studio. Para obtener más información, consulte Configurar App Protection para Virtual Apps and Desktops.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

Después de comprar esta función, asegúrese de habilitar la licencia de App Protection.

> **Renuncia de responsabilidades:**
>
> Las directivas de App Protection funcionan mediante el filtrado del acceso a las funciones requeridas del sistema operativo subyacente (llamadas a API específicas necesarias para capturar pantallas o pulsaciones de teclas). De este modo, las directivas de App Protection pueden proporcionar protección incluso contra herramientas de piratas informáticos personalizadas y diseñadas específicamente. Sin embargo, a medida que los sistemas operativos evolucionan, es posible que surjan nuevas formas de capturar pantallas y registrar pulsaciones de teclas. Si bien seguimos identificándolas y abordándolas, no podemos garantizar una protección completa en configuraciones e implementaciones específicas.
>
> Las directivas de App Protection que ofrece Citrix funcionan con componentes subyacentes del sistema operativo, incluidos los archivos ICA. Citrix podría no ofrecer asistencia si se detectan alteraciones o modificaciones intencionadas de los componentes subyacentes, con lo que se recomienda proporcionar la integridad de las directivas aplicadas.

Comprobar si App Protection está instalada

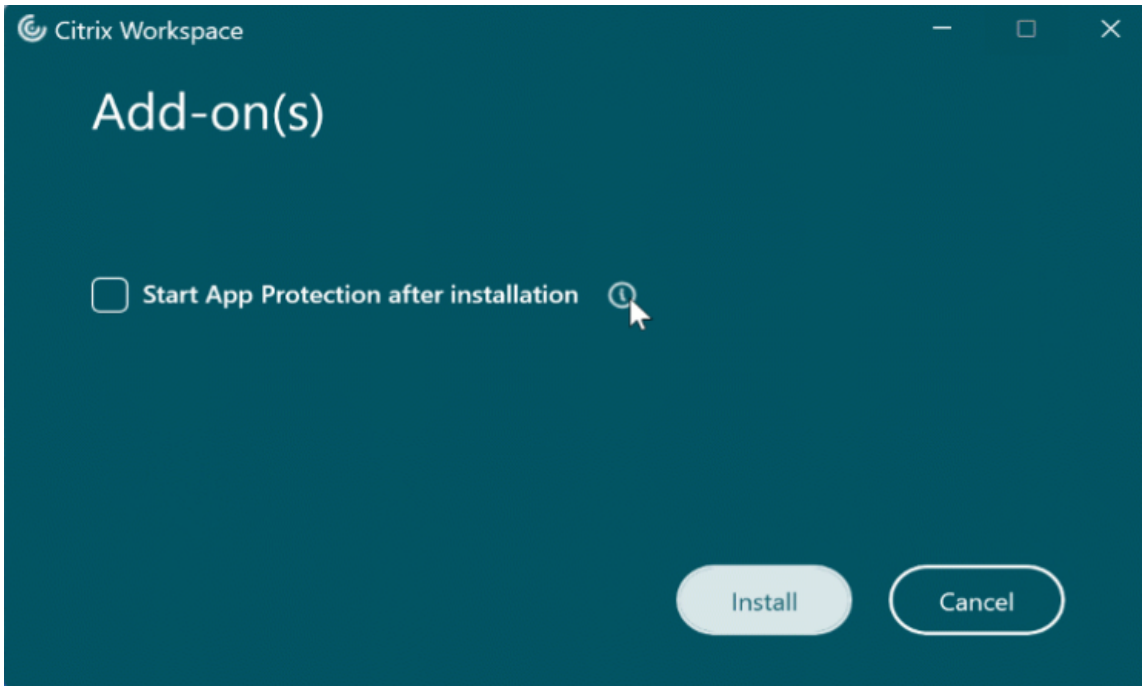
Aplicación Citrix Workspace para Windows

A partir de la versión 2212 de la aplicación Citrix Workspace, App Protection se instala de forma predeterminada. Sin embargo, es posible que el componente esté activo o inactivo según si el usuario marcó la casilla **Iniciar App Protection después de la instalación**.

- Para las versiones de la aplicación Citrix Workspace anteriores a la 2311:

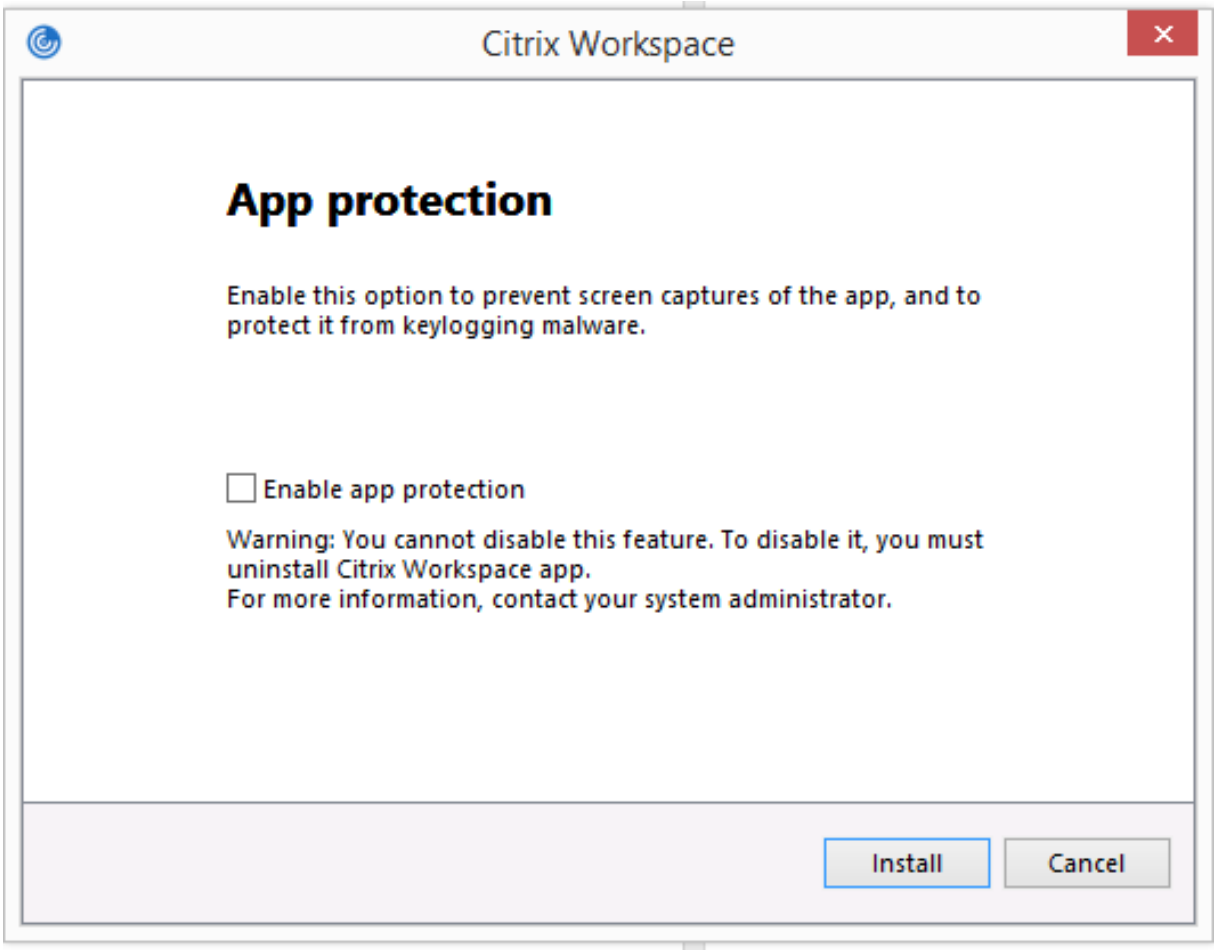
© 1999–2024 Cloud Software Group, Inc. All rights reserved.

- A partir de la versión 2311 de la aplicación Citrix Workspace:



Para las versiones de la aplicación Citrix Workspace anteriores a la 2212, App Protection se instala y está en estado activo solo si marca la casilla **Habilitar App Protection** al instalar la aplicación Citrix Workspace.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.



El estado de App Protection puede ser **DETENIDO** o **EN EJECUCIÓN**.

Para comprobar el estado del servicio, lleve a cabo uno de estos pasos:

- Para la versión 2206 de la aplicación Citrix Workspace o una posterior, ejecute este comando:

```
sc query appprotectionsvc
<!--NeedCopy-->
```

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

```
Command Prompt
Microsoft Windows [Version 10.0.19044.2604]
(c) Microsoft Corporation. All rights reserved.

C:\WINDOWS\system32>sc query appprotectionsvc

SERVICE_NAME: appprotectionsvc
        TYPE               : 10  WIN32_OWN_PROCESS
        STATE              : 4  RUNNING
                                (STOPPABLE, NOT_PAUSABLE, IGNORES_SHUTDOWN)
        WIN32_EXIT_CODE    : 0  (0x0)
        SERVICE_EXIT_CODE  : 0  (0x0)
        CHECKPOINT         : 0x0
        WAIT_HINT          : 0x0

C:\WINDOWS\system32>
```

- Para las versiones de la aplicación Citrix Workspace anteriores a la 2206, ejecute este comando:

```
sc query entryprotectsvc
<!--NeedCopy-->
```

```
C:\Users\[redacted]>sc query entryprotectsvc

SERVICE_NAME: entryprotectsvc
        TYPE               : 10  WIN32_OWN_PROCESS
        STATE              : 4  RUNNING
                                (STOPPABLE, NOT_PAUSABLE, IGNORES_SHUTDOWN)
        WIN32_EXIT_CODE    : 0  (0x0)
        SERVICE_EXIT_CODE  : 0  (0x0)
        CHECKPOINT         : 0x0
        WAIT_HINT          : 0x0
```

> **Nota:**
>
> En las versiones de la aplicación Citrix Workspace anteriores a la 2212, si no se marcó la casilla **Habilitar App Protection** al instalar la aplicación Citrix Workspace ni se ejecutó el comando anterior para comprobar el estado, se muestra este mensaje de error:
>
> ```
> C:\Windows\system32>sc query appprotectionsvc
> [SC] EnumQueryServicesStatus:OpenService FAILED 1060:
>
> The specified service does not exist as an installed service.
> ```

Comportamiento de App Protection en diferentes entornos

El comportamiento de App Protection depende de cómo acceda a los recursos configurados con las directivas de App Protection. Estos recursos incluyen Virtual Apps and Desktops, aplicaciones web

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

internas y aplicaciones SaaS. Puede acceder a estos recursos a través de un explorador web o un cliente de la aplicación Citrix Workspace nativo compatible. App Protection funciona de forma diferente según el entorno:

- **Citrix Receivers o aplicaciones Citrix Workspace no compatibles**: Los recursos configurados con directivas de App Protection no están disponibles.
- **Versiones de la aplicación Citrix Workspace compatibles**: Los recursos configurados con directivas de App Protection están disponibles y se inician correctamente.
- **Inicio híbrido mediante la URL de almacén de Workspace**: Los recursos configurados con directivas de App Protection están siempre disponibles. Para iniciar correctamente los recursos en un explorador web mediante la URL de almacén de Workspace, consulte App Protection para el inicio híbrido de Workspace.
- **Inicio híbrido mediante la URL de almacén de StoreFront**: Los recursos configurados con directivas de App Protection no están disponibles si no se implementa la personalización de StoreFront. Para iniciar correctamente los recursos en un explorador web mediante la URL de almacén de StoreFront, consulte App Protection para el inicio híbrido con StoreFront.

La protección se aplica en las siguientes condiciones:

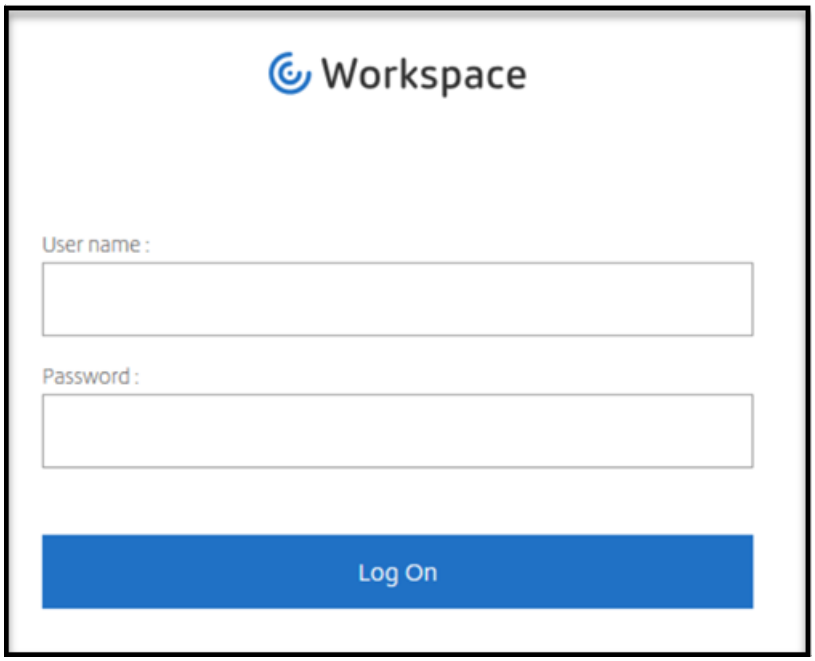
- **Protección contra capturas de pantalla**: En la aplicación Citrix Workspace para Windows y Citrix Workspace para Mac, está habilitada si hay alguna ventana protegida visible en la pantalla. Para inhabilitar la protección, minimice todas las ventanas protegidas. En el caso de la aplicación Citrix Workspace para Linux, está habilitada si hay alguna ventana protegida activa. Para inhabilitar la protección, cierre todas las ventanas protegidas.
- **Protección contra el registro de tecleo**: Habilitada si hay una ventana protegida enfocada. Para inhabilitar la protección, cambie el foco a otra ventana.

¿Qué protege App Protection?

App Protection protege estas ventanas de Citrix:

- Inicio de sesión de Citrix en Windows

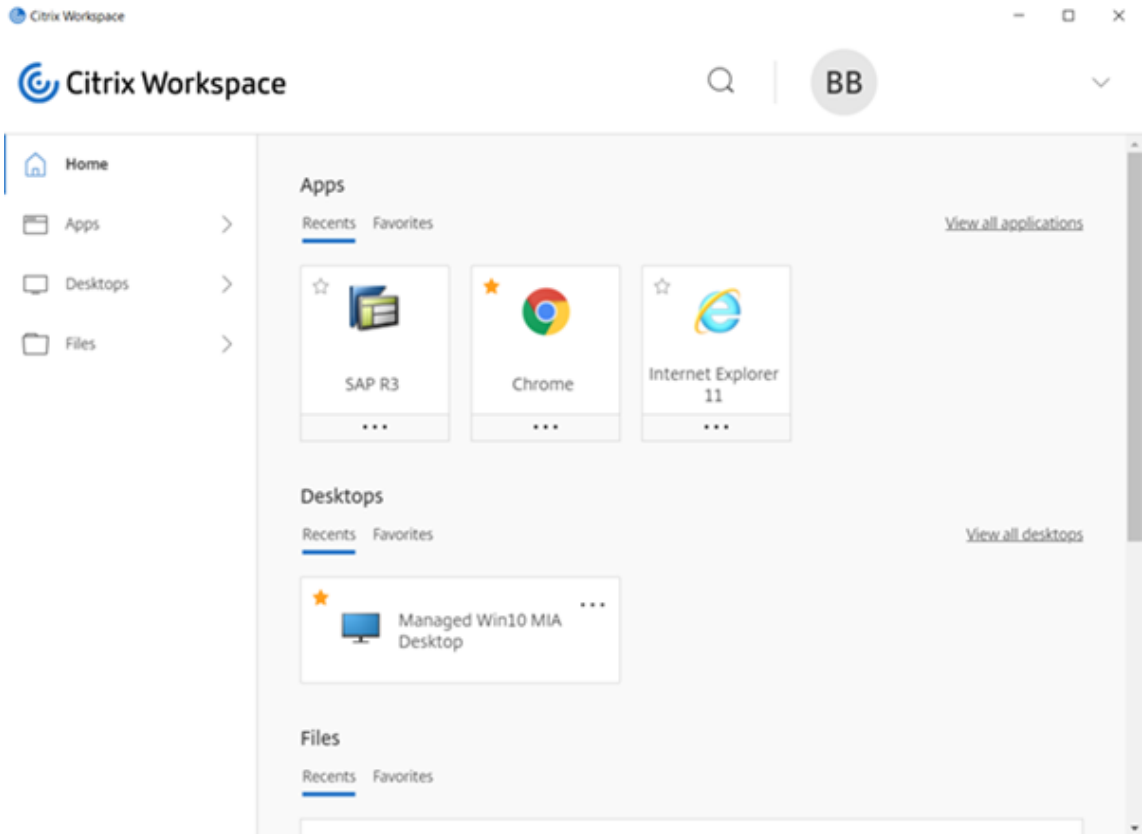
© 1999–2024 Cloud Software Group, Inc. All rights reserved.



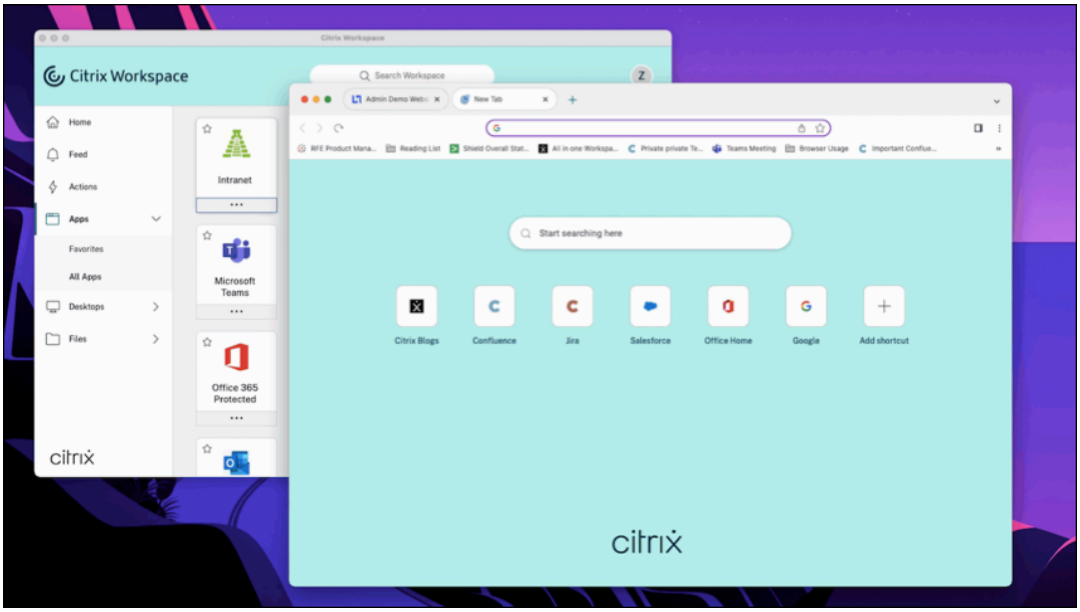
- Ventanas de sesión HDX de la aplicación Citrix Workspace (ejemplo, escritorio administrado)

- Ventanas de autoservicio (almacén)

© 1999–2024 Cloud Software Group, Inc. All rights reserved.



- Aplicaciones web y SaaS
  - Aplicación Citrix Workspace para Windows y aplicación Citrix Workspace para Mac: las aplicaciones web y SaaS se abren en el Citrix Enterprise Browser. Si las aplicaciones están configuradas para usar las directivas de App Protection a través de Citrix Secure Private Access, App Protection se aplica a cada una de las fichas.



© 1999–2024 Cloud Software Group, Inc. All rights reserved.

  - Aplicación Citrix Workspace para Linux: el Citrix Enterprise Browser no es compatible.

¿Qué no protege App Protection?

- Estos elementos que se encuentran bajo el icono de aplicaciones de Citrix Workspace en la barra de navegación:
  - Central de conexiones
  - Todos los enlaces en Preferencias avanzadas
  - Personalizar
  - Comprobar actualizaciones
  - Cerrar sesión
- Si opta por proteger un escritorio virtual con una función de protección contra capturas de pantalla, los usuarios podrán seguir compartiendo la pantalla desde las aplicaciones del escritorio virtual. Sin embargo, en el caso de las aplicaciones que estén fuera del escritorio virtual, no es posible hacer capturas de pantalla ni grabar el escritorio virtual.

Limitaciones

Existen las siguientes limitaciones por diseño:

- Aplicaciones y escritorios virtuales habilitados para App Protection no se pueden iniciar al acceder a ellos desde sesiones de RDP.
- App Protection no está disponible en casos de doble salto y saltos múltiples.
- App Protection no es compatible si tiene una versión no compatible de la aplicación Citrix Workspace o Citrix Receiver. En ese caso, los recursos están ocultos.
- Cuando las funciones de App Protection se aplican a aplicaciones y escritorios virtuales, el uso compartido de la pantalla saliente puede verse afectado si se utiliza la optimización.
- Es posible que la aplicación Citrix Workspace con App Protection no sea compatible con otras aplicaciones o soluciones de seguridad que empleen una tecnología subyacente similar.
- App Protection no es compatible cuando se inician recursos desde Citrix Secure Browser o con Remote Browser Isolation.
- En la aplicación Citrix Workspace para Linux, no puede usar aplicaciones snap cuando está instalada App Protection.

Contextual App Protection

Contextual App Protection ofrece la posibilidad de aplicar directivas de App Protection de forma condicional a un subconjunto de usuarios, en función de sus características, sus dispositivos y la estrategia de red. Para obtener más información, consulte estos artículos:

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

- Contextual App Protection para StoreFront
- Contextual App Protection para Workspace

App Protection para el inicio híbrido

El inicio híbrido de Citrix Virtual Apps and Desktops tiene lugar al iniciar sesión en la aplicación Citrix Workspace a través del explorador (Citrix Workspace para Web) y utilizar las aplicaciones a través de la aplicación Citrix Workspace nativa. El término híbrido hace referencia al uso combinado de la aplicación Citrix Workspace para Web y la aplicación Citrix Workspace nativa para conectar y usar los recursos. La App Protection admite el inicio híbrido en Workspace y StoreFront. Para obtener más información, consulte estos artículos:

- App Protection para inicio híbrido con Workspace
- App Protection para el inicio híbrido con StoreFront

Requisitos del sistema y compatibilidad

April 10, 2024

Requisitos del sistema

Como requisito previo, asegúrese de haber instalado la aplicación Citrix Workspace con derechos de administrador.

Versiones mínimas de los componentes de Citrix

- Aplicación Citrix Workspace 2108 para Linux
- Aplicación Citrix Workspace 2203.1 LTSR para Windows
- Aplicación Citrix Workspace 2002 para Windows
- Aplicación Citrix Workspace 2305.1 para la Tienda Windows
- Aplicación Citrix Workspace 2001 para Mac
- StoreFront 1912 LTSR
- Delivery Controller 1912
- Licencias de Citrix válidas. Para obtener más información, contacte con un representante de Ventas o Citrix Partner.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

> **Nota:**
>
> Si los usuarios utilizan dispositivos o versiones de la aplicación Workspace que no admiten App Protection, no pueden acceder a los recursos protegidos. Los recursos protegidos incluyen Virtual Apps and Desktops y aplicaciones web y SaaS.

Licencias

En la siguiente sección se explican los diferentes tipos de licencias disponibles para App Protection en función de los productos, las plataformas y los casos de uso.

VDI administradas por TI Para todas las ediciones de VDI administradas por TI, la App Protection está disponible como complemento. Para obtener más información, consulte IT-managed VDI.

Citrix DaaS para hiperescaladores

- Azure
- Google
- AWS

Citrix DaaS En el artículo Feature Matrix for Citrix DaaS, vaya a **DaaS Cloud Services > Security and Monitoring > App Protection**.

Citrix Secure Private Access App Protection está disponible como una función adjunta independiente para Citrix Secure Private Access. Para obtener más información, vaya a **Citrix Cloud Services > Citrix Secure Private Access** en el artículo Service descriptions for Citrix Services.

Suscripción de Citrix Universal App Protection se incluye en estos servicios:

- Citrix Universal Premium
- Citrix Universal Premium Plus

Está disponible como complemento en estas ediciones:

- Citrix Universal Advanced
- Citrix Universal Advanced Plus

Para obtener más información, consulte este artículo.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

Plataformas de sistemas operativos

El runtime de directivas de App Protection se instala en el dispositivo de punto final *de origen* y no en el VDA *de destino*. Por lo tanto, solo la versión del sistema operativo del dispositivo de punto final es importante. (App Protection se puede conectar a agentes VDA alojados en cualquier sistema operativo compatible descrito en Requisitos del sistema de Citrix Virtual Apps and Desktops).

La función de App Protection es compatible con dispositivos de punto final que tienen estos sistemas operativos:

- **Windows:**
  - Windows 11 (edición de 64 bits)
  - Windows 10 (ediciones de 32 y 64 bits)

    > **Nota:**
    >
    > App Protection no es compatible con los dispositivos que usan la edición Arm64 del sistema operativo Windows.

- **macOS:**
  - High Sierra (10.13) y versiones posteriores
- **Linux:**
  - Ubuntu 22.04 de 64 bits
  - RHEL 9 de 64 bits
  - Sistema operativo ARM64 Raspberry Pi (basado en Debian 11 (bullseye))

> **Nota:**
>
> Para App Protection, la aplicación Citrix Workspace para Linux requiere un Gnome Display Manager además de los sistemas operativos compatibles.

Tabla de compatibilidad

Tabla de compatibilidad para productos basados en Citrix Cloud

Estas son las funciones de App Protection compatibles con productos basados en Citrix Cloud:

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

Función	Citrix Cloud	Citrix Cloud Japan
Protección contra el registro de tecleo y contra las capturas de pantalla para aplicaciones y escritorios virtuales	Sí	Sí
Protección contra el registro de tecleo y contra las capturas de pantalla para aplicaciones web o SaaS	Sí	No
Protección contra DLL para Windows	Sí	Sí, mediante un objeto de directiva de grupo (GPO)
Lista de permisos para la protección contra DLL	Sí	Sí, a través de GPO
Global App Configuration Service (GACS)	Sí	No
Protección de pantalla para la autenticación y el Self-service Plug para Linux	Sí	Sí, a través de AuthManConfig.xml
Protección de pantalla para la autenticación y el Self-service Plug para Mac	Sí, a través de GACS	Sí, a través de GACS
Protección de pantalla para la autenticación y el Self-service Plug para Windows	Sí	Sí, a través de GPO
Eventos de captura de pantalla de App Protection de CAS	Sí	No
Contextual App Protection	Sí	Sí, según el usuario
Detección de manipulación de directivas	Sí	Sí
Verificación de postura de App Protection	Sí	Sí
Filtro o lista de aplicaciones locales permitidas: Windows	Sí	Sí, a través de GPO
App Protection local: Windows	Sí	Sí, a través de GPO

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

Funciones de App Protection

April 25, 2024

En este artículo se destacan las funciones de App Protection compatibles con la aplicación Citrix Workspace para Windows, la aplicación Citrix Workspace para Linux y la aplicación Citrix Workspace para Mac.

Protección contra el registro de tecleo

A través del cifrado, las funciones contra el registro del tecleo de App Protection codifican el texto que el usuario escribe tanto en el teclado físico como en el de pantalla. La protección contra el registro de tecleo cifra el texto antes de que una herramienta pueda acceder a él desde el nivel del kernel o sistema operativo. Un registrador de las pulsaciones de teclas instalado en el dispositivo de punto final del cliente que leyera los datos del sistema operativo o un controlador capturaría el texto cifrado en lugar de las pulsaciones de teclas del usuario. Las directivas de App Protection están activas no solo para las aplicaciones y los escritorios publicados, sino también para los cuadros de diálogo de autenticación de Citrix Workspace. Su instancia de Citrix Workspace está protegida desde el momento en que los usuarios abren el primer cuadro de diálogo de autenticación. App Protection codifica las pulsaciones de teclas y devuelve texto indescifrable a los programas de registro de tecleo.

Los administradores pueden optar por habilitar la protección contra el registro de tecleo para los siguientes tipos de recursos:

- Escritorios y aplicaciones virtuales
- Aplicaciones web y SaaS internas
- Pantallas de autenticación
- Pantallas de Self-service Plug-in (SSP)

Anticapturas de pantalla

La protección contra capturas de pantalla impide que una aplicación intente hacer una captura o grabación de la pantalla en una sesión de escritorio o aplicación virtual. El software de captura de pantalla no puede detectar contenido dentro de la región de captura. El área seleccionada por la aplicación se muestra atenuada o la aplicación no captura nada, en lugar de la sección de la pantalla que prevé copiar. La función de protección contra capturas de pantalla protege frente a Snip & Sketch, la herramienta
Recortes y **Mayús+Ctrl+Impr Pant** en Windows.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

Otro caso de uso de la función de protección contra capturas de pantalla es impedir que se comparta información confidencial en aplicaciones de reuniones virtuales o conferencias web como GoToMeeting, Microsoft Teams o Zoom. App Protection impide que se comparta información de forma involuntaria, mostrando una pantalla en blanco en las conferencias web cuando las aplicaciones están protegidas. Esta función garantiza que la información confidencial no se filtre accidentalmente de la organización. Esta función ayuda a cumplir con la normativa en sectores regulados, puesto que la intención no se tiene en cuenta al revelarse una filtración de datos.

Los administradores pueden optar por habilitar la protección contra capturas de pantalla para los siguientes tipos de recursos:

- Escritorios y aplicaciones virtuales
- Aplicaciones web y SaaS internas
- Pantallas de autenticación
- Pantallas de Self-service Plug-in (SSP)

> **Nota:**
>
> Si ha iniciado dos escritorios virtuales y uno de ellos está habilitado con la función de protección contra captura de pantalla y el otro no, la función de protección contra captura de pantalla se aplicará a ambos escritorios virtuales. No puede realizar una captura de pantalla de ninguno de los escritorios virtuales.
>
> En caso de que haya minimizado el escritorio virtual que está habilitado con la protección contra captura de pantalla, la función de protección contra captura de pantalla seguirá aplicándose al escritorio virtual que no tiene dicha función.

Detección y notificación de capturas de pantalla

Con la aplicación Citrix Workspace, podrá ver una notificación cuando haya un posible intento de captura de pantalla con relación a cualquier recurso protegido. Para obtener información sobre los recursos protegidos con App Protection, consulte ¿Qué protege App Protection?

La notificación aparece cuando hay:

- Un intento de hacer una captura de pantalla o grabar un vídeo a través de una herramienta para captura de pantallas.
- Un intento de hacer una captura de pantalla con la tecla Imprimir pantalla.

> **Nota:**
>
> - La notificación aparece solo una vez por instancia en ejecución de la herramienta de captura de pantallas. La notificación se muestra de nuevo si se vuelve a iniciar la herramienta y se intenta capturar la pantalla.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

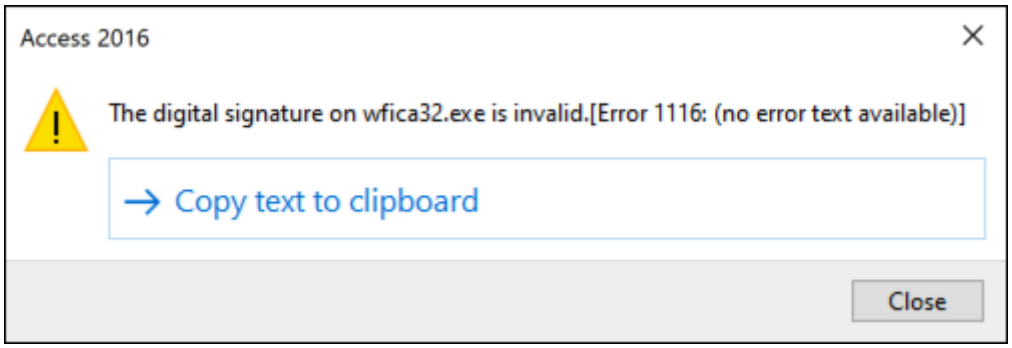
> - En la aplicación Citrix Workspace para Windows 2212 y versiones posteriores, las ventanas de inicio de sesión y las ventanas de autoservicio (Tienda) no están protegidas de forma predeterminada.

Antiinyección de DLL

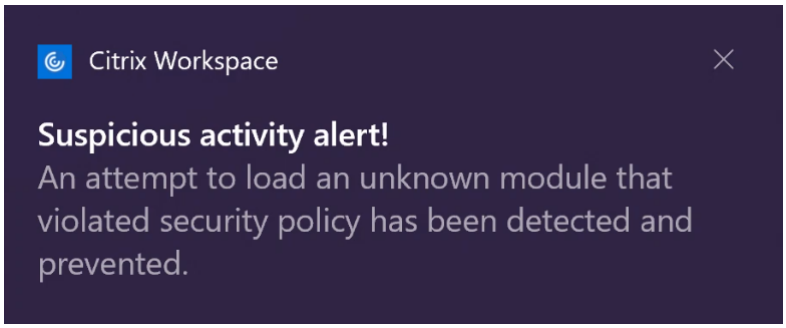
La mejora de seguridad antiinyección de DLL ayuda a proteger la aplicación Citrix Workspace frente determinadas bibliotecas de enlace dinámico (DLL) no autorizadas o frente a módulos que no son de confianza. Si se inyectan estos módulos que no son de confianza, la aplicación Citrix Workspace detecta estas intervenciones e impide que los módulos se carguen. Además, si se detecta alguna DLL maliciosa o que no sea de confianza antes del inicio de la sesión, App Protection bloquea el inicio de la sesión y muestra un mensaje de error. Al cerrar el mensaje de error, se cierra la sesión de escritorio y aplicación virtual.

Esta función está disponible con todas las aplicaciones y escritorios virtuales protegidos y con la ventana de autenticación de la aplicación Citrix Workspace (implementación local o StoreFront).

La mejora cierra la sesión inmediatamente cuando existen determinadas DLL maliciosas o que no son de confianza en el componente protegido



La mejora muestra una notificación cuando se bloquea una DLL maliciosa o que no es de confianza. Al cerrar el mensaje, se cierra la sesión de escritorio y aplicación virtual.



Aviso: Esta característica funciona mediante el filtrado del acceso a las funciones necesarias del sistema operativo subyacente (llamadas a API específicas necesarias para cargar las DLL). De este modo,

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

puede proporcionar protección incluso contra ciertas herramientas de piratas informáticos personalizadas y diseñadas específicamente. Sin embargo, a medida que los sistemas operativos evolucionan, pueden surgir nuevas formas de cargar archivos DLL. Si bien seguimos identificándolas y abordándolas, no podemos garantizar una protección completa en configuraciones e implementaciones específicas.

Esta función es compatible con la aplicación Citrix Workspace para Windows 2206 y versiones posteriores.

> **Nota:**
>
> Anteriormente, las funcionalidades de protección contra la captura de tecleo y contra las capturas de pantalla se aplicaban de forma predeterminada para la autenticación de Citrix y las pantallas de la aplicación Citrix Workspace. Sin embargo, a partir de 2212, estas capacidades están inhabilitadas de forma predeterminada y deben configurarse mediante el objeto de directiva de grupo. Para obtener información sobre la configuración del objeto de directiva de grupo, consulte Mejora de la configuración de App Protection.

Compatibilidad con la optimización de HDX para Microsoft Teams

Microsoft Teams optimizado permite el uso compartido de la pantalla cuando la aplicación Citrix Workspace está habilitada con App Protection únicamente en el modo Desktop Viewer. Al hacer clic en **Compartir contenido** en Microsoft Teams, el selector de pantallas ofrece estas opciones:

- La opción **Ventana** para compartir aplicaciones abiertas: Esta opción solo se muestra si la versión del VDA es 2109 o una posterior.
- La opción **Escritorio** para compartir el contenido del escritorio del VDA: esta opción solo se muestra en las siguientes versiones de la aplicación Citrix Workspace:
  - Aplicación Citrix Workspace para Linux 2311 o una versión posterior
  - Aplicación Citrix Workspace para Mac 2308 o una versión posterior
  - Aplicación Citrix Workspace para Windows versión 2309 o posterior

> **Nota:**
>
> En la aplicación Citrix Workspace para Linux, la opción de compartir escritorio está inhabilitada de forma predeterminada. Para habilitarla, agregue el parámetro `UseGbufferScreenSharing` en su archivo *config.json* de la siguiente manera:
>
> ```
> mkdir -p /var/.config/citrix/hdx_rtc_engine
> vim /var/.config/citrix/hdx_rtc_engine/config.json
> {
>
>  "UseGbufferScreenSharing":1
>  }
> ```

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

```
7
8 <!--NeedCopy-->
```

Microsoft Teams optimizado con App Protection habilitada también permite el diseño de monitores virtuales de Citrix, con el que puede compartir cada monitor virtual de forma individual.

> **Limitación:**
>
> - Microsoft Teams optimizado con App Protection habilitada no presenta compatibilidad con el uso compartido de la pantalla en escritorios publicados habilitados con acceso a aplicaciones locales (LAA).
> - El contenido generado por el cliente, como el contenido del explorador web mediante BCR, no se puede capturar ni compartir. Si intenta realizar una captura de pantalla, se mostrará como una pantalla negra.
>
> **Nota:**
>
> En el caso de la aplicación Citrix Workspace para Linux, esta función se encuentra en Technical Preview.

App Protection local (Technical Preview)

App Protection ofrece una mayor seguridad a la hora de defender a los clientes de registradores de pulsaciones de teclas y capturas de pantalla, ya sean accidentales o maliciosas, en los dispositivos de punto final. Actualmente, las funciones de App Protection solo se ofrecen con los recursos de Workspace. Con esta función, las funciones de App Protection se extienden a las aplicaciones locales residentes en los dispositivos de punto final. A partir de la aplicación Citrix Workspace 2210 para Windows, se puede aplicar App Protection a las aplicaciones locales de los dispositivos Windows.

Regístrese en la versión Technical Preview de esta función mediante el formulario de Podio.

Detección de manipulación de directivas

La función de detección de manipulación de directivas impide que el usuario acceda a sesiones de escritorio o aplicación virtual si se alteran las directivas de App Protection de protección contra capturas de pantalla y el registro de tecleo. Si se detecta una alteración de las directivas, la sesión de escritorio o aplicación virtual finaliza.

> **Nota:**
>
> La función de detección de manipulación de directivas se inhabilitará de forma predeterminada en una versión futura.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

Para configurar la detección de manipulación de directivas, consulte Configurar la detección de manipulación de directivas.

Verificación de la postura

Para detectar y bloquear el inicio de aplicaciones y escritorios virtuales que están habilitados con directivas de App Protection desde versiones de la aplicación Citrix Workspace que no admiten la función de detección de manipulación de directivas, habilite la Comprobación de la postura de App Protection.

> **Nota:**
>
> Si la comprobación de la postura está habilitada y utiliza la versión de la aplicación Citrix Workspace que no presenta compatibilidad con la comprobación de la postura, las sesiones habilitadas con directivas de App Protection se finalizan.

Para configurar la verificación de la postura, consulte Configurar la verificación de la postura.

> **Limitación:**
>
> La comprobación de la postura deja de funcionar de forma intermitente cuando se utilizan VDA en estaciones de trabajo con Windows alojadas en Microsoft Azure.

Caso de App Protection con DoubleHop

Las funciones de App Protection no están disponibles en casos de doble salto. “Doble salto”significa una sesión de Citrix Virtual Apps o Virtual Desktops que se ejecuta dentro de una sesión de Citrix Virtual Desktops. Antes, podía iniciar aplicaciones y escritorios virtuales que están habilitados con directivas de App Protection en casos de doble salto, pero las funciones de App Protection no se aplicaban.

A partir de la versión 2309 de la aplicación Citrix Workspace para Windows, presentamos una directiva de grupos de Windows que permite bloquear el inicio de aplicaciones y escritorios virtuales habilitados con directivas de App Protection en casos de doble salto. Para obtener más información sobre cómo habilitar el parámetro **Bloquear inicio de doble salto**, consulte Habilitar el parámetro Bloquear inicio de doble salto.

Servicio Citrix Analytics para App Protection

Cuando usa Citrix Virtual Apps and Desktops, se generan eventos de usuario correspondientes a sus actividades y acciones. Citrix Analytics for Security tiene una función denominada **Búsqueda de autoservicio** que registra esos eventos de usuario y le proporciona insights sobre ellos. La **búsqueda**

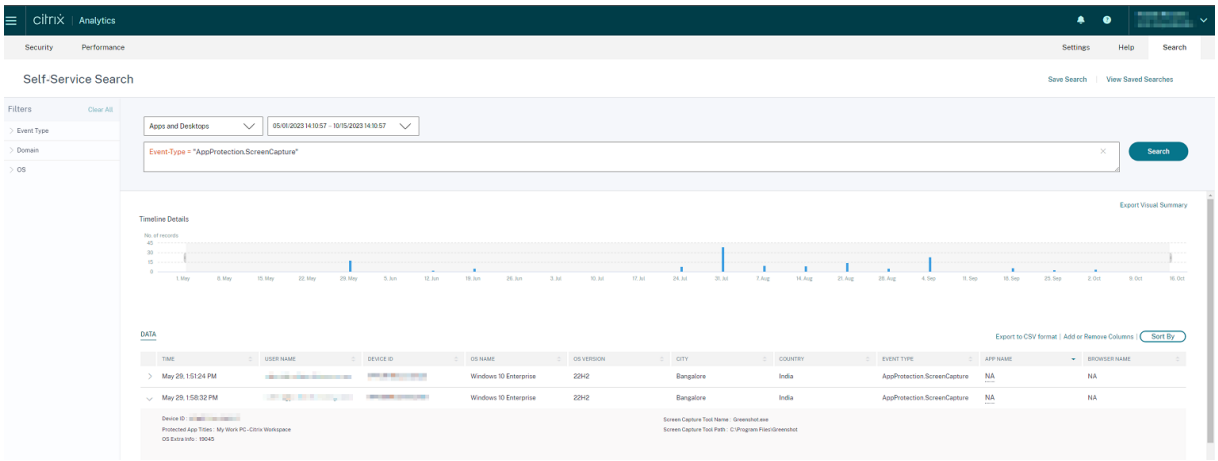
© 1999–2024 Cloud Software Group, Inc. All rights reserved.

de autoservicio le permite buscar, filtrar y explorar esos eventos de usuario para poder comprender qué evento de usuario se lleva a cabo y actuar en función de la gravedad del evento. Para obtener más información sobre la **búsqueda de autoservicio**, consulte Búsqueda de autoservicio.

La **Búsqueda de autoservicio para Apps y Desktops** tiene un tipo de evento `AppProtection.ScreenCapture` que le permite determinar si se intenta realizar capturas de pantalla de las Virtual Apps o Desktops que están habilitados con las directivas de App Protection. Para obtener más información sobre cómo buscar un evento de usuario, consulte Especificar una consulta de búsqueda para filtrar eventos.

Este servicio proporciona la siguiente información:

- ID de dispositivo
- Títulos de aplicaciones protegidas
- Información adicional del sistema operativo
- Nombre de la herramienta de captura de pantalla
- Ruta de la herramienta de captura de pantalla



Lista de permitidos para capturas de pantalla

Si la aplicación Citrix Workspace, las aplicaciones y escritorios virtuales o las aplicaciones SaaS están habilitadas con la directiva anticaptura de pantalla de App Protection, no podrá capturar sus pantallas con ninguna herramienta diseñada para tal fin.

Sin embargo, a partir de la versión 2402 de la aplicación Citrix Workspace para Windows, la función Lista de permitidos para capturas de pantalla le permite agregar una aplicación a la lista de permitidos para capturas de pantalla. Esta función le permite usar la aplicación de la lista de permitidos y capturar la pantalla del recurso habilitado con la directiva anticaptura de pantalla de App Protection. Para agregar una aplicación a la lista de permitidos para capturas de pantalla, consulte Configurar Lista de permitidos para capturas de pantalla.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

> **Importante:**
>
> No se recomienda ejecutar una aplicación incluida en la lista de permitidos en el dispositivo durante un período más prolongado, ya que reduce la postura de seguridad. Puede usar las aplicaciones de la lista de permitidas para compartir su pantalla temporalmente en situaciones como la solución de problemas. Se recomienda cumplir con las siguientes condiciones:
>
> - Ejecute la aplicación incluida en la lista de permitidas durante un período breve junto con el recurso habilitado con la función anticaptura de pantalla de App Protection.
> - Cierre la aplicación incluida en la lista de permitidas inmediatamente después de completar la tarea requerida.
> - Agregue una marca de agua al compartir la pantalla mientras usa el recurso habilitado con la función anticaptura de pantalla de App Protection para mayor seguridad.

Lista de exclusión de procesos

Al iniciar cualquier proceso o aplicación en el dispositivo, las DLL de App Protection se inyectan en cada proceso si App Protection está habilitada. En ocasiones, esto puede provocar que el proceso o la aplicación no funcionen debido a problemas de compatibilidad con la DLL.

A partir de la versión 24.02 de la aplicación Citrix Workspace para Windows, puede agregar cualquier proceso a la lista de exclusión de procesos para evitar que las DLL de App Protection se incorporen a ese proceso en particular y evitar problemas de compatibilidad causados por la presencia de las DLL de App Protection. Para configurar la lista de exclusión de procesos, consulte Configurar Lista de exclusión de procesos.

> **Importante:**
>
> No se recomienda excluir procesos, ya que esto reduce la postura de seguridad. Puede usar esto para desbloquear temporalmente el uso de la aplicación y generar un tíquet de asistencia para una investigación más a fondo.

Lista de exclusión de controladores de filtro USB

A veces, cuando se usan teclados externos especializados, como teclados para juegos, con la aplicación Citrix Workspace, el controlador de filtros USB de App Protection puede provocar problemas de compatibilidad e impedir que el uso del teclado.

A partir de la versión 2402 de la aplicación Citrix Workspace para Windows, la función Lista de exclusión de controladores de filtro USB le permite excluir cualquier dispositivo USB que presente problemas de compatibilidad con la aplicación Citrix Workspace mediante el ID de proveedor y el ID de

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

producto del dispositivo. Para agregar cualquier dispositivo a la Lista de exclusión de controladores de filtro USB, consulte Configurar Lista de exclusión de controladores de filtro USB.

> **Nota:**
>
> No se recomienda excluir dispositivos de forma permanente. Use esta función para impedir de forma temporal que el usuario utilice el dispositivo y generar un tíquet de asistencia para investigar más a fondo el problema de compatibilidad.

Configurar App Protection

April 10, 2024

App Protection proporciona una seguridad mejorada cuando se utiliza la aplicación Citrix Workspace. La función restringe la posibilidad de que los clientes puedan verse amenazados por malware de registro de pulsaciones de teclas y malware de capturas de pantalla. App Protection evita la exfiltración de información confidencial, como credenciales de usuario e información confidencial mostrada en la pantalla. La función evita que los usuarios y los atacantes hagan capturas de pantalla y usen registradores de pulsaciones de teclas para obtener y explotar información confidencial.

En este artículo se explica cómo configurar App Protection en la aplicación Citrix Workspace en diferentes plataformas.

App Protection está disponible en la aplicación Citrix Workspace para las siguientes plataformas:

- Aplicación Citrix Workspace para Windows
- Aplicación Citrix Workspace para Linux
- Aplicación Citrix Workspace para Mac

> **Renuncia de responsabilidades**
>
> Las directivas de App Protection filtran el acceso a las funciones requeridas del sistema operativo subyacente. Se necesitan llamadas a API específicas para capturar pantallas o pulsaciones de teclas. Las directivas de App Protection proporcionan protección incluso contra herramientas de piratas informáticos personalizadas y con un diseño específico. Sin embargo, a medida que los sistemas operativos evolucionan, es posible que surjan nuevas formas de capturar pantallas y registrar pulsaciones de teclas. Si bien seguimos identificándolas y abordándolas, no podemos garantizar una protección completa en configuraciones e implementaciones específicas.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

Aplicación Citrix Workspace para Windows

Requisitos previos

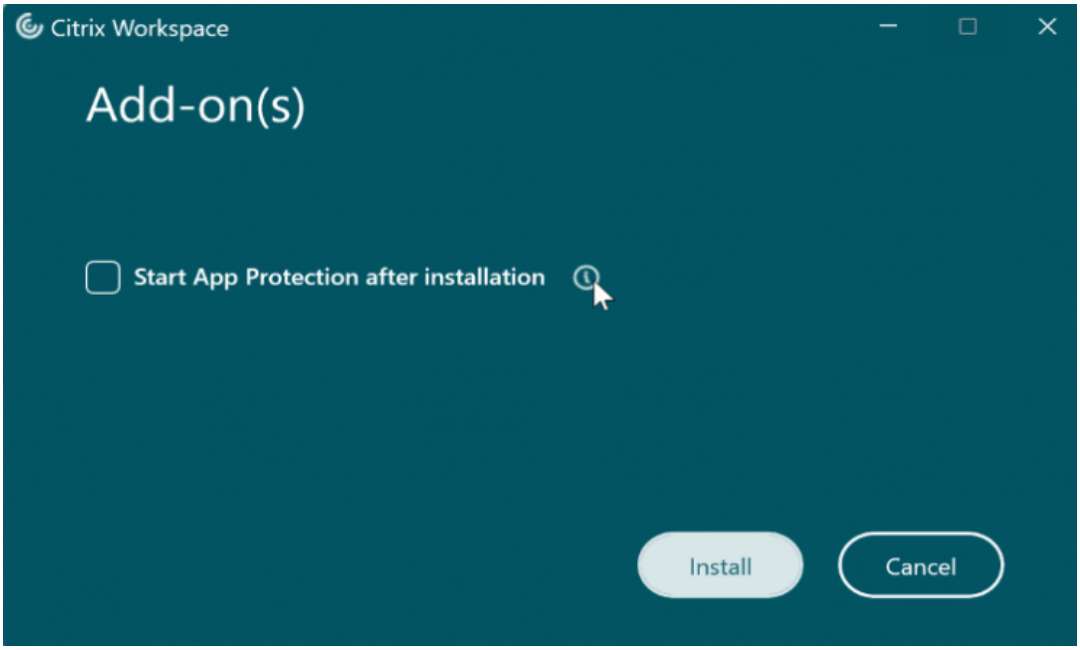
- Citrix Virtual Apps and Desktops 1912 LTSR o versiones posteriores.
- StoreFront versión 1912 LTSR o Workspace.
- Aplicación Citrix Workspace 2203.1 LTSR o una versión posterior.
- Una licencia de App Protection válida.
- A partir de la versión 2212 de la aplicación Citrix Workspace, el componente App Protection se instala de forma predeterminada durante la instalación de la aplicación Citrix Workspace.

  La casilla de verificación **Habilitar App Protection** que se muestra durante la instalación se sustituye por **Iniciar App Protection después de la instalación**.

  - Para las versiones de la aplicación Citrix Workspace anteriores a la 2311:

  - A partir de la versión 2311 de la aplicación Citrix Workspace:

© 1999–2024 Cloud Software Group, Inc. All rights reserved.



Al seleccionar esta casilla de verificación, App Protection se inicia inmediatamente después de la instalación.

> **Nota:**
>
> Si no se habilita esta casilla de verificación, App Protection se inicia automáticamente al iniciar por primera vez un recurso o componente protegido en el caso de los clientes que tienen derechos para usar el componente App Protection.

Configurar

Configure las siguientes funciones de App Protection para la aplicación Citrix Workspace para Windows:

- **Protección contra el registro de tecleo y capturas de pantalla:**
  - Para Virtual Apps and Desktops, consulte Configurar la protección contra el registro de tecleo y capturas de pantalla para Virtual Apps and Desktops.
  - Para las aplicaciones web y SaaS, consulte Configurar la protección contra el registro de tecleo y capturas de pantalla para las aplicaciones web y SaaS.
  - Para la autenticación y Self-service Plug-in:
    - Mediante la interfaz de usuario del Global App Configuration Service, consulte Configurar la protección contra el registro de tecleo y capturas de pantalla para la autenticación y el Self-service Plug-in mediante la interfaz de usuario de Global App Configuration Service

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

  * Mediante un objeto de directiva de grupo, consulte Configurar la protección contra el registro de tecleo y capturas de pantalla para la autenticación y el Self-service Plug-in mediante un objeto de directiva de grupo
  * Mediante la API, consulte Configurar la protección contra el registro de tecleo y capturas de pantalla para la autenticación y el Self-service Plug-in mediante una API de GACS

- Para configurar la función antiinyección de DLL, consulte Configurar la función antiinyección de DLL.
- Para configurar la manipulación de directivas de App Protection, consulte Configurar la manipulación de directivas de App Protection.
- Para configurar la Comprobación de la postura de App Protection, consulte Configurar comprobación de la postura de App Protection.
- Para habilitar el parámetro de inicio de doble salto, consulte Bloquear inicio de doble salto.

Limitaciones

- Esta función solo está disponible en sistemas operativos de escritorio como Windows 11 y Windows 10.
- A partir de la versión 2006.1, la aplicación Citrix Workspace no se admite en Windows 7. Por lo tanto, App Protection no funciona en Windows 7. Para obtener más información, consulte Elementos retirados.
- Esta función no se puede usar con el Protocolo de escritorio remoto (RDP).

Interfaz de línea de comandos

Puede iniciar el componente App Protection mediante el parámetro `/startappprotection` de línea de comandos. Sin embargo, el conmutador `/includeappprotection` anterior se ha retirado.

La tabla siguiente proporciona información sobre las pantallas protegidas en función de la implementación:

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

Implementación de App Protection	Pantallas protegidas	Pantallas no protegidas
Se incluye en la aplicación Citrix Workspace	Cuadro de diálogo de credenciales de usuario / administrador de autenticación y Self-service Plug-in	Central de conexiones, Dispositivos, mensajes de error de la aplicación Citrix Workspace, Reconexión automática de clientes, Agregar cuenta
Se ha configurado en el Controller	Pantalla de sesión ICA (tanto aplicaciones como escritorios)	Central de conexiones, Dispositivos, mensajes de error de la aplicación Citrix Workspace, Reconexión automática de clientes, Agregar cuenta

Al tomar una captura de pantalla, solo se oscurece la ventana protegida. Puede hacer una captura de pantalla de la zona que queda fuera de la ventana protegida. Sin embargo, si utiliza la tecla **Impr Pant** para hacer una captura de pantalla en un dispositivo con Windows 10, debe minimizar la ventana protegida.

Anteriormente, las funcionalidades de protección contra la captura de tecleo y contra las capturas de pantalla se aplicaban de forma predeterminada para la autenticación de Citrix y las pantallas de la aplicación Citrix Workspace. Sin embargo, a partir de 2212, estas capacidades están inhabilitadas de forma predeterminada y deben configurarse mediante el objeto de directiva de grupo.

> **Nota:**
>
> Esta directiva de GPO no se aplica a las sesiones ICA y SaaS. Las sesiones ICA y SaaS se siguen controlando mediante el Delivery Controller y Citrix Secure Private Access.

Mejora en App Protection:

A partir de la versión 2305 de la aplicación Citrix Workspace para Windows, se habilita la protección contra el registro de tecleo en las pantallas de autenticación y del Self-service Plug-in si se cumple uno de estos criterios:

- Habilitó App Protection mediante una de estas opciones:
  - Marcar la casilla **Iniciar App Protection** durante la instalación.
  - Iniciar el componente App Protection mediante el parámetro **/startappprotection** de la línea de comandos.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

- Si no marcó la casilla de verificación **Iniciar App Protection** ni utilizó el parámetro de línea de comandos **/startappprotection** durante la instalación, la protección contra el registro de tecleo se habilitará tras iniciar el primer recurso protegido.

> **Nota:**
>
> Global App Configuration Service y los objetos de directiva de grupo (GPO) supeditan el comportamiento anterior. Por ejemplo, si inhabilitó GACS o la directiva de GPO para estas pantallas, la protección contra el registro de tecleo no estará habilitada en las pantallas de autenticación y SSP.

Aplicación Citrix Workspace para Linux

A partir de la versión 2108, la función App Protection es completamente funcional. Esta función es compatible con Virtual Apps and Desktops y está habilitada de forma predeterminada. Sin embargo, debe configurar la función de App Protection en el archivo `AuthManConfig.xml` para habilitarla en las interfaces del administrador de autenticación y del Self-service Plug-in.

Requisito previo

App Protection funciona mejor con estos sistemas operativos y GNOME Display Manager:

- Ubuntu 18.04, Ubuntu 20.04 y Ubuntu 22.04 de 64 bits
- Debian 9 y Debian 10 de 64 bits
- CentOS 7 de 64 bits
- RHEL 7 de 64 bits
- Sistema operativo Raspberry Pi (Buster) con armhf de 32 bits (basado en Debian 10)
- Sistema operativo ARM64 Raspberry Pi (basado en Debian 11 (bullseye))

> **Nota:**
>
> Si usa una versión de la aplicación Citrix Workspace anterior a 2204, la función de App Protection no es compatible con los sistemas operativos que usa n `glibc` 2.34 o una versión posterior.
>
> Si instala la aplicación Citrix Workspace con la función App Protection habilitada en un SO que usa `glibc`2.34 o una versión posterior, es posible que, al reiniciar el sistema, el SO no arranque. Para recuperarse de un error de arranque del SO, realice una de estas acciones:
>
> - Instale de nuevo el sistema operativo.
> - Vaya al modo de recuperación del sistema operativo y desinstale la aplicación Citrix Workspace desde el terminal.
> - Arranque el sistema desde el SO en directo y quite el archivo `rm -rf /etc/ld.so.`

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

> `preload` del SO existente.

Instalación del componente de App Protection

1. Al instalar la aplicación Citrix Workspace con el paquete tarball, aparece el siguiente mensaje: **¿Quiere instalar el componente de App Protection? Advertencia: No puede inhabilitar esta función. Para inhabilitarla, debe desinstalar la aplicación Citrix Workspace. Para obtener más información, póngase en contacto con el administrador de sistemas. [default $INSTALLER_N]:**
2. Presione **Y** para instalar el componente de App Protection. App Protection no se instala de forma predeterminada.
3. Reinicie la máquina para que se reflejen los cambios. App Protection funciona como es debido solamente tras reiniciar la máquina.

Instalación del componente de App Protection en paquetes RPM A partir de la versión 2104, App Protection se ofrece en la versión RPM de la aplicación Citrix Workspace.

Para instalar App Protection, haga esto:

1. Al instalar la aplicación Citrix Workspace.
2. Instale el paquete `ctxappprotection<version>.rpm` de App Protection desde el instalador de la aplicación Citrix Workspace.
3. Reinicie el sistema para que se reflejen los cambios.

Instalar el componente de App Protection en paquetes Debian A partir de la versión 2101, App Protection se ofrece en la versión Debian de la aplicación Citrix Workspace.

Para instalar el componente de App Protection, ejecute el siguiente comando desde el terminal antes de instalar la aplicación Citrix Workspace:

```
export DEBIAN_FRONTEND="noninteractive"
sudo debconf-set-selections <<< "icaclient app_protection/
    install_app_protection select yes"

sudo debconf-show icaclient
* app_protection/install_app_protection: yes

sudo apt install -f ./icaclient_<version>._amd64.deb
<!--NeedCopy-->
```

A partir de la versión 2106, la aplicación Citrix Workspace presenta una opción para configurar las funciones de protección contra el registro de tecleo y protección contra capturas de pantalla por separado para las interfaces del administrador de autenticación y del Self-service Plug-in.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

Configurar

Configure las siguientes funciones de App Protection para la aplicación Citrix Workspace para Linux:

- Para configurar la protección contra el registro de tecleo y la captura de pantallas para la pantalla de autenticación, consulte Configurar mediante AuthManConfig.xml para Authentication Manager.
- Para configurar la protección contra registro de tecleo y captura de pantallas para la pantalla del Self-service Plug-in, consulte Configurar mediante AuthManConfig.xml para la interfaz del Self-service Plug-in.
- Para configurar la protección contra el registro de tecleo y capturas de pantalla para Virtual Apps and Desktops, consulte Configurar la protección contra el registro de tecleo y capturas de pantalla para Virtual Apps and Desktops.
- Para configurar la manipulación de directivas de App Protection, consulte Configurar la manipulación de directivas de App Protection.
- Para configurar la Comprobación de la postura de App Protection, consulte Configurar comprobación de la postura de App Protection.

Aplicación Citrix Workspace para Mac

Configure las siguientes funciones de App Protection para la aplicación Citrix Workspace para Mac:

- Para configurar la protección contra el registro de tecleo y capturas de pantalla para la autenticación y el Self-service Plug-in mediante la interfaz de usuario del Global App Configuration Service, consulte Configurar la protección contra el registro de tecleo y capturas de pantalla para la autenticación y el Self-service Plug-in mediante la interfaz de usuario de Global App Configuration Service.
- Para configurar la protección contra el registro de tecleo y capturas de pantalla para la autenticación y el Self-service Plug-in mediante una API, consulte Configurar la protección contra el registro de tecleo y capturas de pantallas para la autenticación y el Self-service Plug-in mediante una API de GACS.
- Para configurar la protección contra el registro de tecleo y capturas de pantalla para Virtual Apps and Desktops, consulte Configurar la protección contra el registro de tecleo y capturas de pantalla para Virtual Apps and Desktops.
- Para configurar la protección contra el registro de tecleo y capturas de pantalla para aplicaciones web y SaaS, consulte Configurar la protección contra el registro de tecleo y capturas de pantalla para las aplicaciones web y SaaS.
- Para configurar la manipulación de directivas de App Protection, consulte Configurar la manipulación de directivas de App Protection.
- Para configurar la Comprobación de la postura de App Protection, consulte Configurar comprobación de la postura de App Protection.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

Recomendación

Las directivas de App Protection se centran en mejorar la seguridad y la protección de los dispositivos de punto final. Revise todas las demás recomendaciones y directivas de seguridad de su entorno. Puede utilizar una plantilla de directiva de **Seguridad y control** para la configuración recomendada en entornos con baja tolerancia al riesgo. Para obtener más información, consulte Plantillas de directiva.

Configurar la protección contra el registro de tecleo y capturas de pantalla

April 10, 2024

Puede configurar la protección contra el registro de tecleo y capturas de pantalla para lo siguiente:

- Autenticación y Self-service Plug-in
- Aplicaciones y escritorios virtuales
- Aplicaciones web y SaaS

Configurar la protección contra el registro de tecleo y capturas de pantalla para la autenticación y el Self-service Plug-in

Puede configurar la protección contra el registro de tecleo y capturas de pantalla para la autenticación y el Self-service Plug-in usando los siguientes métodos:

Método de configuración	Aplicación Citrix Workspace para Linux	Aplicación Citrix Workspace para Mac	Aplicación Citrix Workspace para Windows
Mediante un objeto de directiva de grupo	No	No	Sí
Uso de Global App Configuration Service	No	Sí	Sí
Uso de AuthManConfig.xml	Sí	No	No

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

Mediante un objeto de directiva de grupo

1. Ejecute `gpedit.msc` para abrir la plantilla administrativa de GPO de la aplicación Citrix Workspace.
2. En el nodo **Configuración del equipo**, vaya a **Plantillas administrativas** > **Componentes de Citrix** > **Citrix Workspace**.
3. En función de si configura App Protection para el Authentication Manager o el Self-service Plug-in, siga uno de estos pasos:
   - **Administrador de autenticación**
     Para configurar la protección contra el registro de tecleo y la protección contra capturas de pantalla para el administrador de autenticación, seleccione **Autenticación de usuarios** > directiva **Administrar App Protection**.
   - **Interfaz del Self-service Plug-in**
     Para configurar la protección contra el registro de tecleo y la protección contra capturas de pantalla para la interfaz del Self-service Plug-in, seleccione **Autoservicio** > directiva **Administrar App Protection**.
4. Seleccione una de estas opciones o las dos:
   - **Protección contra el registro de tecleo**: Evita que programas capturen tecleo.
   - **Protección contra capturas de pantalla**: Evita que los usuarios realicen capturas de pantalla y compartan su pantalla.
5. Haga clic en **Aplicar** y **Aceptar**.

Comportamiento previsto:

El comportamiento previsto depende del método por el cual accede al almacén de StoreFront que tiene los recursos protegidos.

Uso de la interfaz de usuario de Global App Configuration Service

A partir de las versiones 2302 o 2301 de la aplicación Citrix Workspace para Windows, estas permiten configurar App Protection para las pantallas de autenticación y Self-service Plug-in mediante Global App Configuration Service (GACS).

Si habilita las funciones de protección contra el registro de tecleo y capturas de pantalla mediante el GACS, se aplicarán tanto a las pantallas de autenticación como a las de Self-service Plug-in.

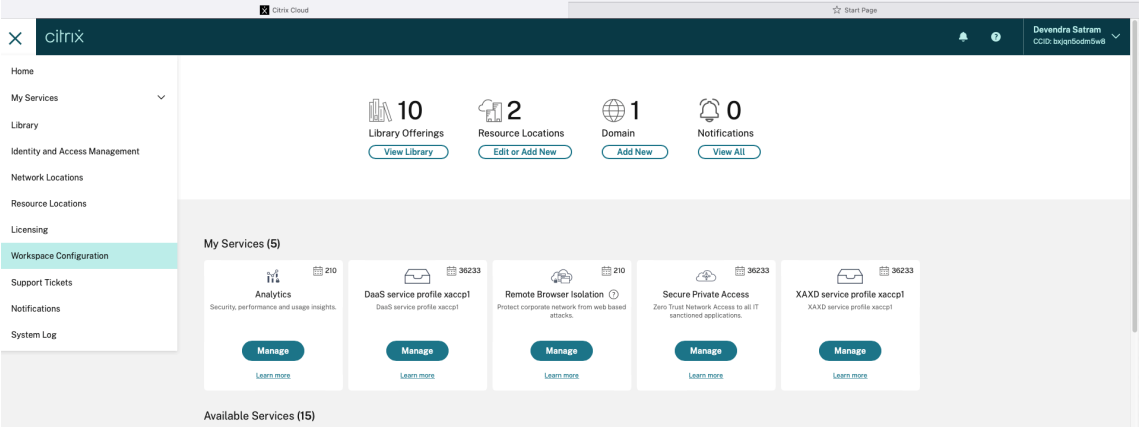
> **Nota:**
>
> - La protección contra el registro de tecleo y capturas de pantalla para la autenticación y el Self-service Plug-in mediante GACS es aplicable a las aplicaciones Citrix Workspace para

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

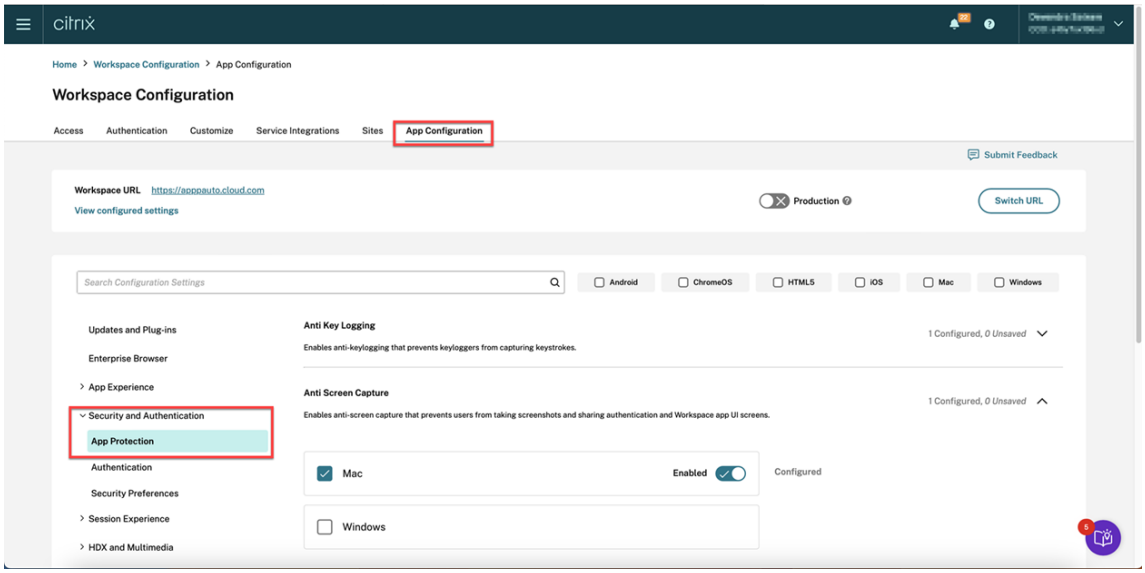
> Windows y Citrix Workspace para Mac. No se aplica a la aplicación Citrix Workspace para Linux.
> - Las configuraciones de GACS no se aplican a Virtual Apps and Desktops ni a las aplicaciones web y SaaS. Estos recursos se siguen controlando mediante el Delivery Controller y Citrix Secure Private Access.
> - A partir de la versión 2311 de la aplicación Citrix Workspace para Mac, se puede configurar App Protection para la autenticación y Self-service Plug-in mediante la interfaz de usuario de Global App Configuration Service para almacenes en la nube y localmente. Sin embargo, si usa la aplicación Citrix Workspace para Mac anterior a la versión 2311, solo puede configurarla para almacenes en la nube.

Los administradores pueden configurar App Protection mediante la interfaz de usuario de Configuración de Workspace:

1. Inicie sesión en su cuenta de Citrix Cloud y seleccione **Configuración de Workspace**.

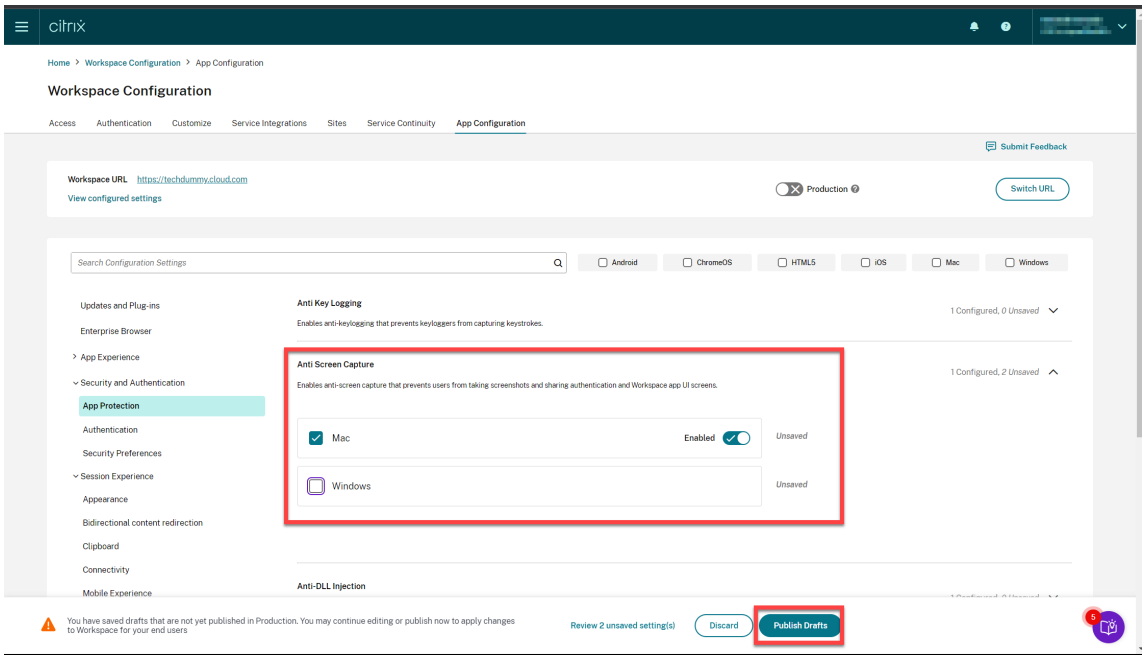


2. Seleccione **Configuración de la aplicación** > **Seguridad y autenticación** > **App Protection**.

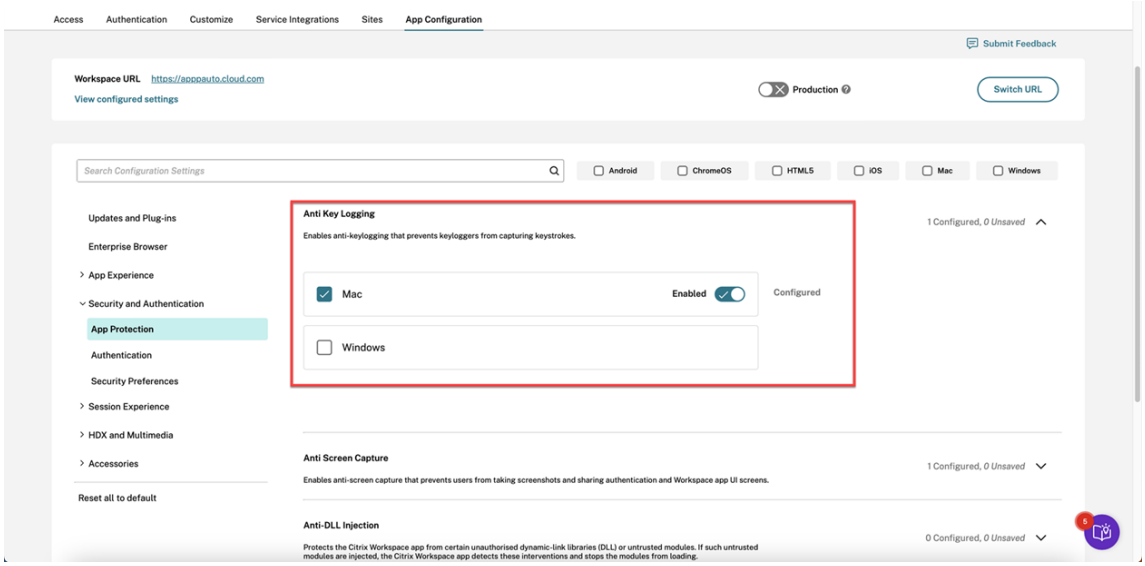


© 1999–2024 Cloud Software Group, Inc. All rights reserved.

3. Haga clic en **Protección contra capturas de pantalla** y, a continuación, seleccione el sistema operativo correspondiente (Windows o Mac).
4. Haga clic en el botón **Habilitado** y, a continuación, en **Publicar borradores**.

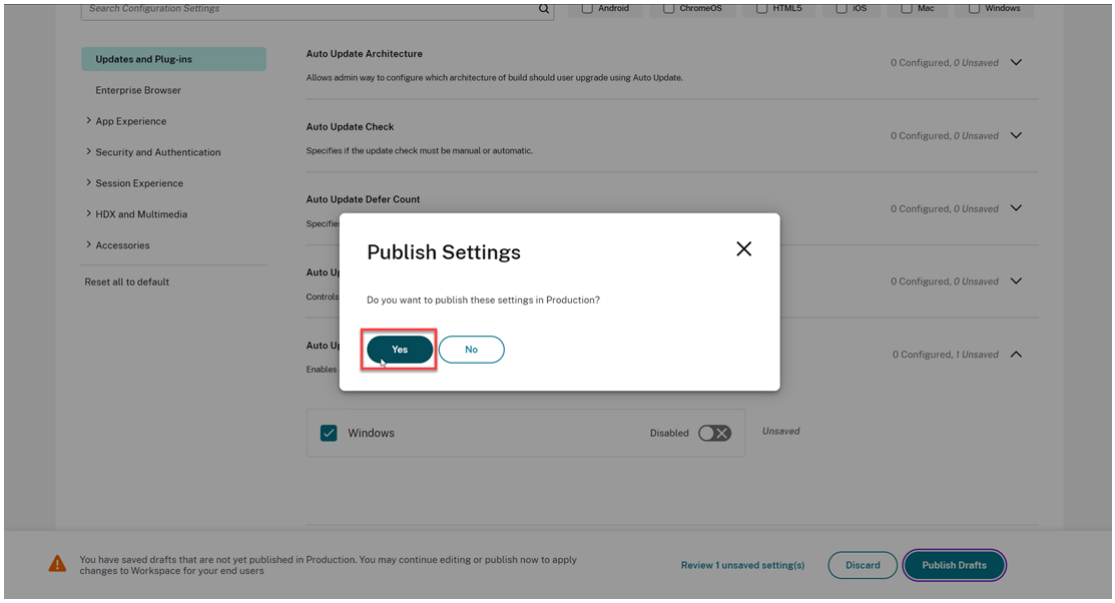


5. Haga clic en **Protección contra tecleo** y, a continuación, seleccione el sistema operativo correspondiente (Windows o Mac).
6. Haga clic en el botón **Habilitado** y, a continuación, en **Publicar borradores**.



7. En el cuadro de diálogo **Parámetros de publicación**, haga clic en **Sí**.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.



Uso de la API de Global App Configuration Service

Los administradores pueden usar la API para configurar estas funciones de App Protection. Los parámetros son los siguientes:

- **Configuración para habilitar o inhabilitar la protección contra capturas de pantalla:**

  “nombre”: “enable anti screen capture for auth and ssp”
  “valor”: “true”o “false”

- **Configuración para habilitar o inhabilitar la protección contra el registro de tecleo:**

  “nombre”: “enable anti key-logging for auth and ssp”
  “valor”: “true”o “false”

Ejemplo: A continuación se incluye un archivo JSON de ejemplo para habilitar las funciones de protección contra capturas de pantalla y contra el registro de tecleo para la aplicación Citrix Workspace en GACS:

```
1  {
2
3
4          "category": "App Protection",
5
6          "userOverride": true,
7
8          "assignedTo": [
9
10           "AllUsersNoAuthentication"
11
12         ],
```

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

```
13
14          "settings": [
15
16            {
17
18
19              "name": "enable anti screen capture for auth and ssp",
20
21              "value": true
22
23             }
24  ,
25
26            {
27
28
29              "name": "enable anti key-logging for auth and ssp",
30
31              "value": true
32
33             }
34
35
36          ] }
```

Uso de AuthManConfig.xml para un Authentication Manager

Vaya a `$ICAROOT/config/AuthManConfig.xml` y modifique el archivo de esta manera:

```
1 /opt/Citrix/ICAClient/config$ cat AuthManConfig.xml | grep -i
    authmananti -A 1
2     <key>AuthManAntiScreenCaptureEnabled</key>
3     <value>true</value>
4     <key>AuthManAntiKeyLoggingEnabled</key>
5     <value>true </value>
6
7 <!--NeedCopy-->
```

Uso de AuthManConfig.xml para la interfaz del Self-service Plug-in

Vaya a `$ICAROOT/config/AuthManConfig.xml` y modifique el archivo de esta manera:

```
1 /opt/Citrix/ICAClient/config$ cat AuthManConfig.xml | grep -i
    protection -A 4
2 <!-- Selfservice App Protection configuration -->
3     <Selfservice>
4       <AntiScreenCaptureEnabled>true</AntiScreenCaptureEnabled>
5       <AntiKeyLoggingEnabled>true</AntiKeyLoggingEnabled>
6     </Selfservice>
```

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

```
7
8 <!--NeedCopy-->
```

Configurar la protección contra el registro de tecleo y capturas de pantalla para Virtual Apps and Desktops

Dos directivas proporcionan funciones de protección contra el registro de tecleo y las capturas de pantalla en las sesiones. Puede configurar la protección contra el registro de tecleo y capturas de pantalla para Virtual Apps and Desktops de la siguiente manera:

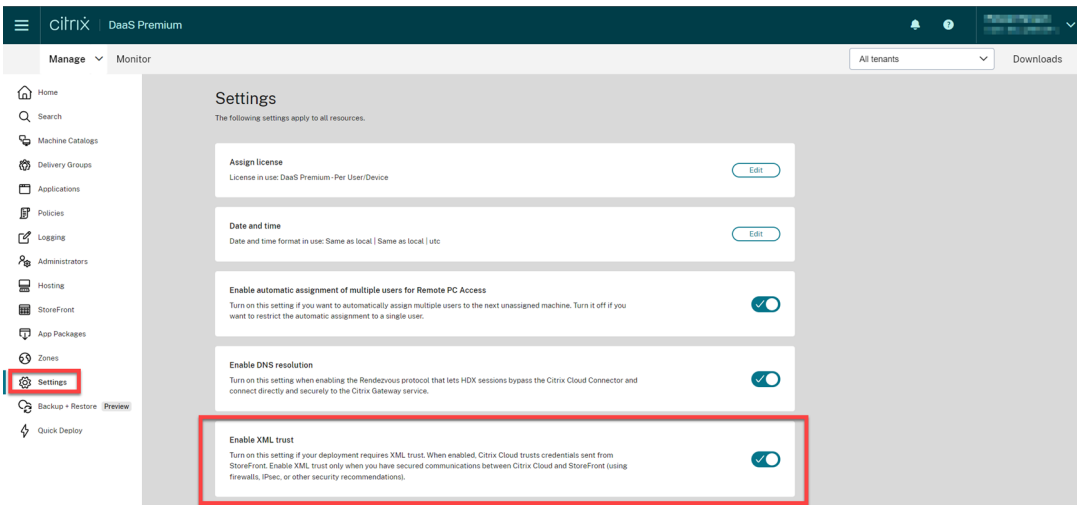
> **Nota:**
>
> A partir de la versión 2103, Citrix DaaS ofrece App Protection con StoreFront y Workspace.

Mediante Web Studio

Para configurar la protección contra el registro de tecleo y la captura de pantalla de Citrix Virtual Apps o Desktops a través de Web Studio, lleve a cabo los siguientes pasos:

1. App Protection requiere confianza en XML. Para habilitar la confianza en XML, lleve a cabo los siguientes pasos:

   a) Inicie sesión en su cuenta de Citrix DaaS y vaya a **Administrar** > **Parámetros** > **Habilitar la confianza en XML**.



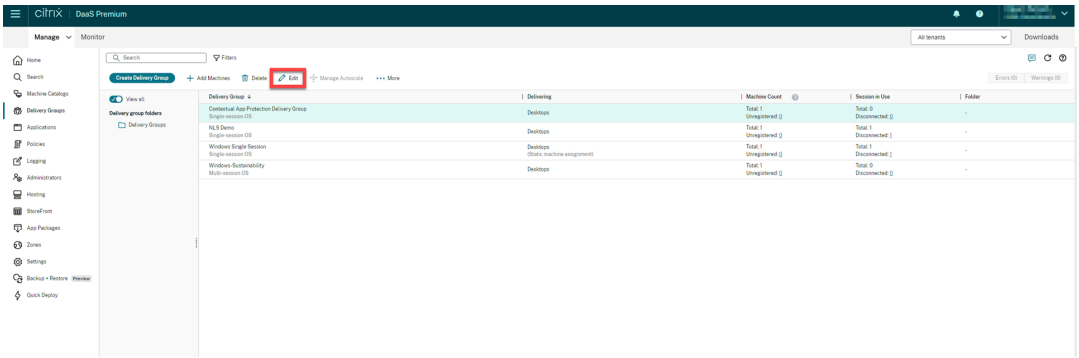
   b) Active la opción **Habilitar confianza en XML**.

2. Para elegir un método de App Protection para un grupo de entrega, siga estos pasos:

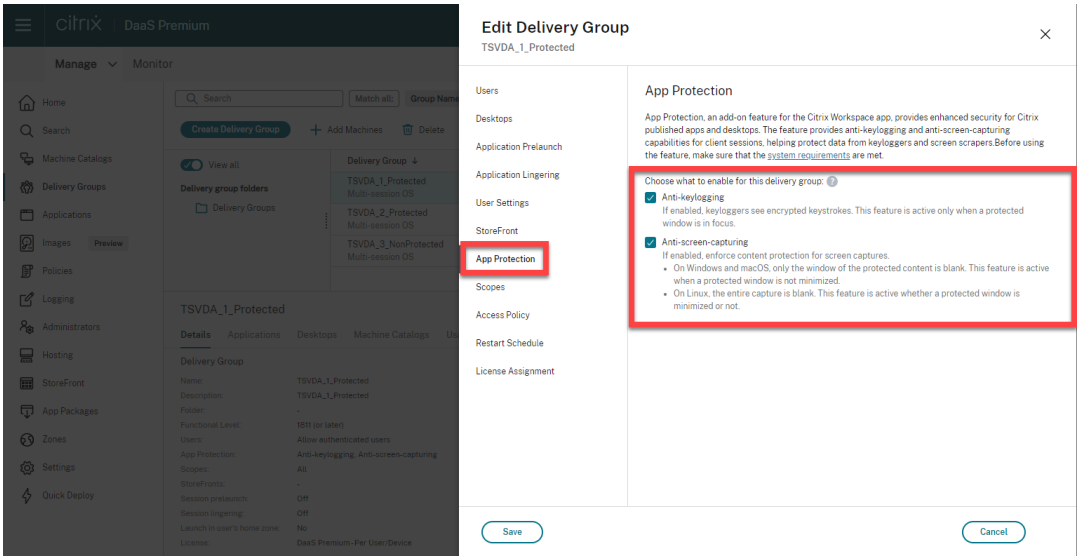
   a) En Citrix DaaS, vaya a **Administrar** > **Grupos de entrega**.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

b) Seleccione un grupo de entrega y, a continuación, haga clic en **Modificar** en la barra de acciones.



c) Haga clic en **App Protection** y, a continuación, seleccione las casillas de verificación **Protección contra el registro de tecleo** y **Protección contra la captura de pantalla**.



d) Haga clic en **Guardar**.

Mediante PowerShell

> **Nota:**
>
> En un entorno de Citrix DaaS, utilice los cmdlets del SDK de PowerShell remoto de Citrix Virtual Apps and Desktops en cualquier máquina (aparte de las máquinas con Citrix Cloud Connectors) para ejecutar los comandos de esta sección.

Habilite estas propiedades para el grupo de entrega con App Protection mediante el SDK de Citrix Virtual Apps and Desktops en cualquier máquina con un Delivery Controller instalado o en una máquina con una versión autónoma de Studio que tenga instalados los complementos FMA de PowerShell.

- `AppProtectionKeyLoggingRequired`: `True`

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

- `AppProtectionScreenCaptureRequired`: `True`

Puede habilitar cada una de estas directivas individualmente por grupo de entrega. Por ejemplo: puede configurar la protección contra el registro de tecleo solo para DG1 y la protección contra capturas de pantalla solo para DG2. Puede habilitar ambas directivas para DG3.

Ejemplo:

Para habilitar ambas directivas para un grupo de entrega denominado **DG3**, ejecute el siguiente comando en cualquier Delivery Controller del sitio:

```
Set-BrokerDesktopGroup -Name DG3 -AppProtectionKeyLoggingRequired
$true -AppProtectionScreenCaptureRequired $true
```

Para validar los parámetros, ejecute este cmdlet:

```
Get-BrokerDesktopGroup -Property Name, AppProtectionKeyLoggingRequired
, AppProtectionScreenCaptureRequired | Format-Table -AutoSize
```

Además, habilite la confianza en XML:

```
Set-BrokerSite -TrustRequestsSentToTheXmlServicePort $true
```

Asegúrese de proteger la red entre StoreFront y el intermediario. Para obtener más información, consulte los artículos CTX236929 y Securing the XenApp and XenDesktop XML Service de Knowledge Center.

Configurar la protección contra tecleo y capturas de pantalla para aplicaciones web y SaaS

Las aplicaciones web y SaaS se abren en el Citrix Enterprise Browser para la aplicación Citrix Workspace para Windows y en la aplicación Citrix Workspace para Mac. Si las aplicaciones están configuradas para usar las directivas de App Protection a través de Citrix Secure Private Access, App Protection se aplica a cada una de las fichas.

Configure App Protection para aplicaciones web y SaaS de la siguiente manera:

- Para configurar App Protection para aplicaciones web y SaaS para Workspace, consulte Citrix Secure Private Access para Citrix Workspace.
- Para configurar App Protection para aplicaciones web y SaaS para StoreFront, consulte Compatibilidad de Citrix Secure Private Access con StoreFront.

Configurar la antiinyección de DLL

March 11, 2024

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

De forma predeterminada, la función de antiinyección de DLL está inhabilitada. Puede habilitar esta función de la siguiente manera:

- Objeto de directiva de grupo (GPO)
- Global App Configuration Service (GACS)

Configurar mediante un objeto de directiva de grupo

Se agregan estas directivas para configurar la función de antiinyección de DLL:

- Antiinyección de DLL
- Lista permitida de módulos de antiinyección de DLL

Uso de la directiva de antiinyección de DLL

Use esta directiva para habilitar o inhabilitar la función de antiinyección de DLL. Cuando no se configura esta directiva, se inhabilita la función antiinyección de DLL. Los valores posibles son:

- **Habilitado**: la función antiinyección de DLL se habilita para Citrix Authentication Manager, la interfaz de usuario de la aplicación Citrix Workspace y Citrix Virtual Apps and Desktops. Los administradores pueden seleccionar los componentes necesarios para habilitar la función de antiinyección de DLL.
- **Inhabilitado**: la función antiinyección de DLL se inhabilita para Citrix Authentication Manager, la interfaz de usuario de la aplicación Citrix Workspace y Citrix Virtual Apps and Desktops.

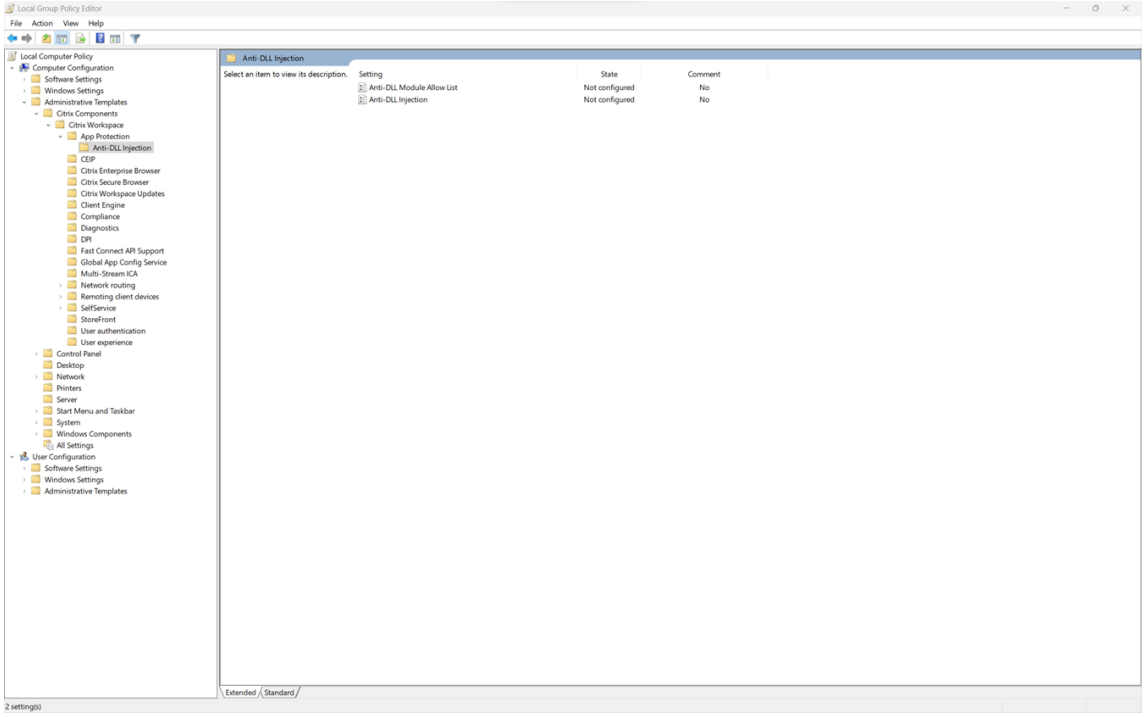
Para habilitar la directiva de antiinyección de DLL, siga estos pasos:

1. Para abrir la plantilla administrativa de objeto de directiva de grupo de la aplicación Citrix Workspace ejecute el siguiente comando:

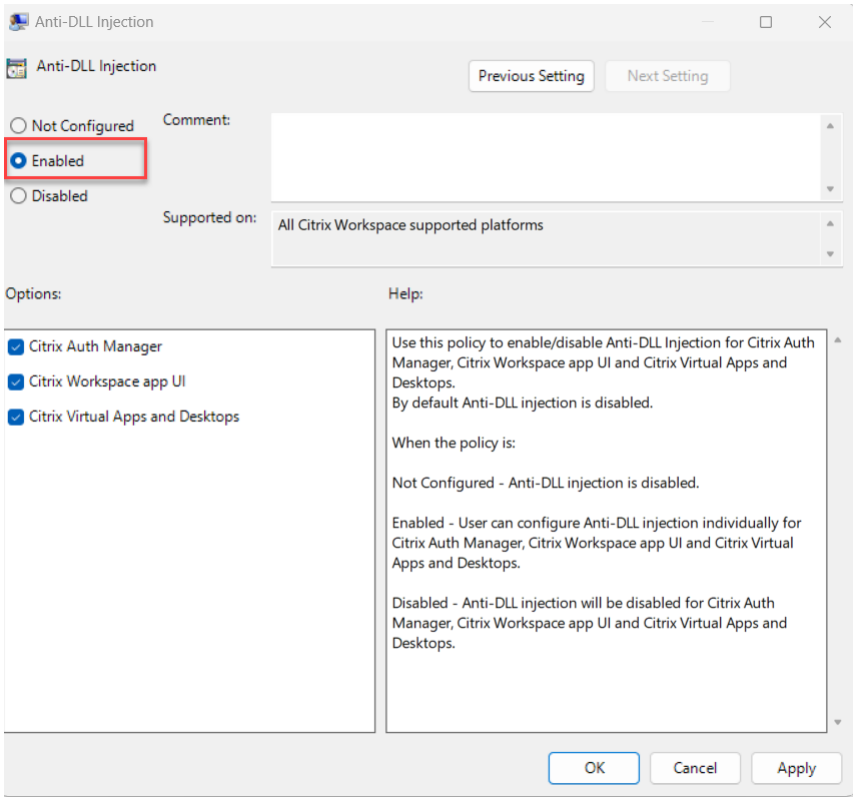
   ```
   gpedit.msc
   ```

2. En el nodo **Configuración del equipo**, vaya a **Plantillas administrativas** > **Componentes de Citrix** > **Citrix Workspace** > **App Protection** > **Antiinyección de DLL**.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.



3. Haga clic en la directiva **Antiinyección de DLL** y seleccione **Habilitado**. Se seleccionan todos los componentes. Sin embargo, puede modificar la selección de los componentes desde la sección Opciones.



© 1999–2024 Cloud Software Group, Inc. All rights reserved.

4. Haga clic en **Aceptar**.

Uso de la directiva de la lista de permitidos del módulo de antiinyección de DLL

Como administrador, puede utilizar esta directiva para excluir cualquier DLL de la función de antiinyección de DLL. Citrix recomienda utilizar esta directiva solo para gestionar situaciones excepcionales. Si esta directiva no se configura, ninguna DLL forma parte de la lista de permitidos. Se incluyen todas las DLL para la protección contra DLL. Los valores posibles son:

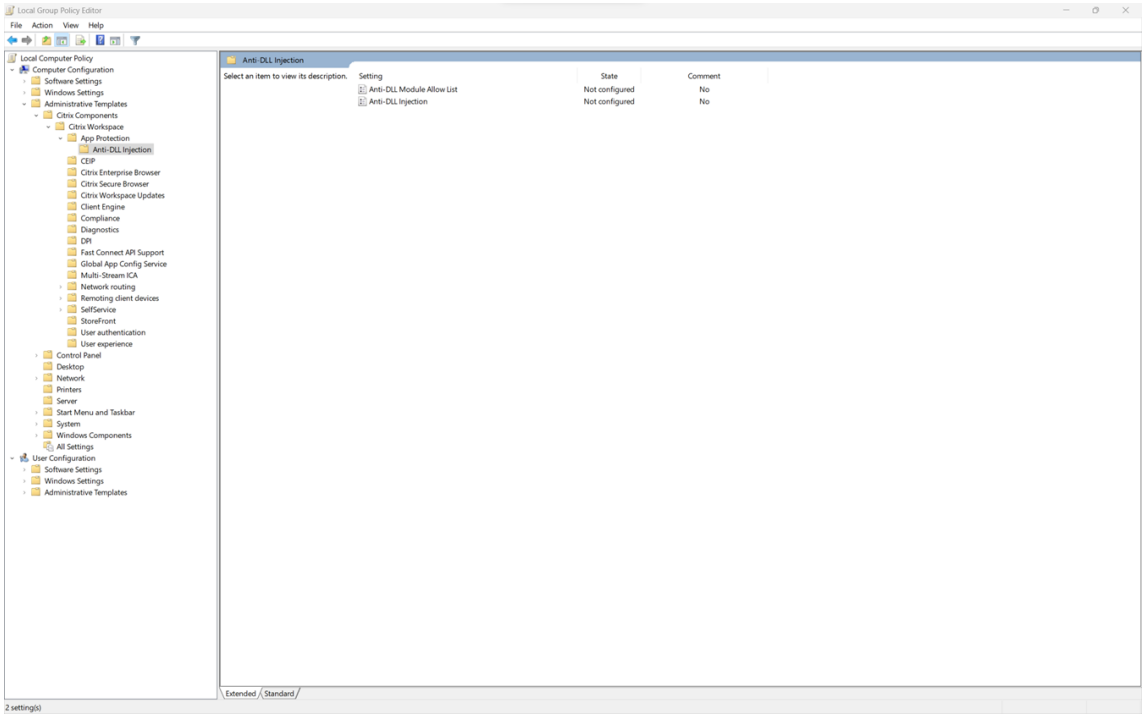
- **Habilitado**: Excluye de la protección contra DLL las DLL que se agregan a la lista de permitidos.
- **Inhabilitado**: Borra la lista de las DLL agregadas a la lista de permitidos.

Para habilitar la directiva de lista de permitidos del módulo de antiinyección de DLL, siga estos pasos:

1. Para abrir la plantilla administrativa de objeto de directiva de grupo de la aplicación Citrix Workspace ejecute el siguiente comando:

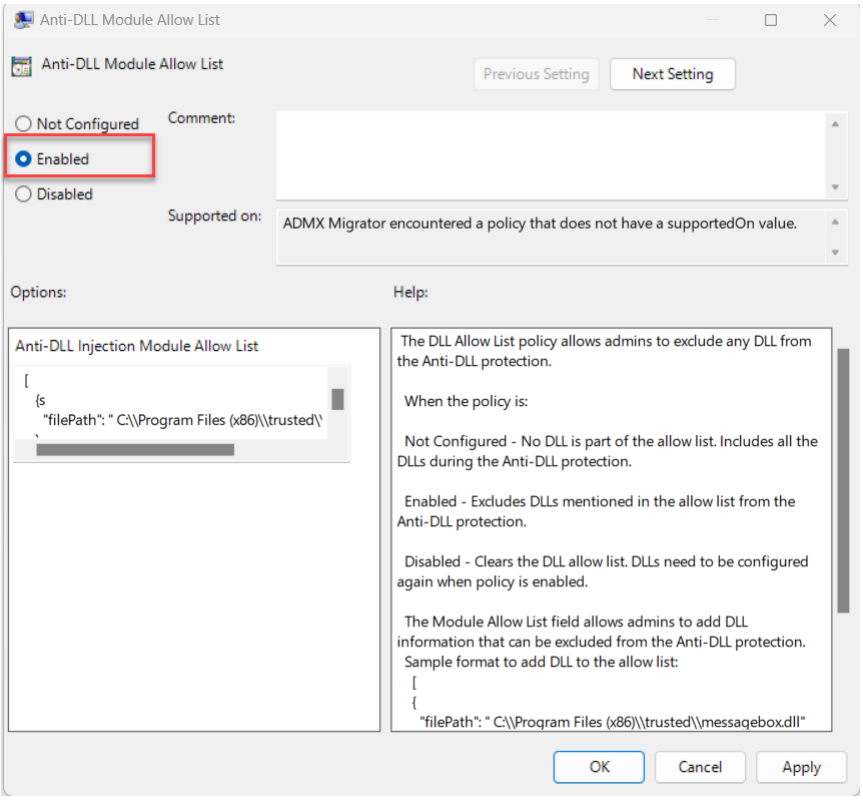
   ```
   gpedit.msc
   ```

2. En el nodo **Configuración del equipo**, vaya a **Plantillas administrativas** > **Componentes de Citrix** > **Citrix Workspace** > **App Protection** > **Lista de módulos permitidos de protección contra DLL**.



3. Haga clic en la directiva **Lista de permitidos del módulo Antiinyección de DLL** y **habilítela**.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.



4. Agregue la lista de módulos que quiere excluir de la protección contra DLL en el campo **Lista de módulos permitidos de protección contra DLL**.
   Formato de ejemplo para agregar DLL a la lista de permitidos:

```
[
    {

        "filePath":"C:\Program Files (x86)\trusted\messagebox.dll"
     }
 ,
    {

        "filePath":"%PROGRAMFILES%\trusted\logging.dll"
     }

]
<!--NeedCopy-->
```

5. Haga clic en **Aceptar**.

Configuración mediante el Global App Configuration Service

Los administradores pueden usar GACS para configurar la función de antiinyección de DLL. Los parámetros son los siguientes:

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

- Antiinyección de DLL: Agregue los módulos necesarios para habilitar la función de antiinyección de DLL.
- Lista de módulos permitidos de protección contra DLL: agregue las DLL necesarias que quiera excluir de la protección contra DLL

Para obtener más información, consulte Global App Configuration Service.

A continuación se muestra un archivo JSON de ejemplo para habilitar la **antiinyección de DLL** y la **lista de permisos del módulo Antiinyección de DLL** para la aplicación Citrix Workspace para Windows en GACS:

```
{

  "serviceURL": {

    "url": "https://tuleshtest.cloudburrito.com:443"
   }
 ,
  "settings": {

    "appSettings": {

      "windows": [
        {

          "category": "App Protection",
          "userOverride": false,
          "assignedTo": [
            "AllUsersNoAuthentication"
          ],
          "assignmentPriority": 0,
          "settings": [
            {

              "name": "anti dll injection",
              "value": [
                "Citrix Auth Manager",
                "Citrix Virtual Apps And Desktops",
                "Citrix Workspace app UI"
              ]
             }
 ,
            {

              "name": "anti dll module allow list",
              "value": [
                {

                  "filePath": "C:\Program Files (x86)\Citrix\ICA Client
                      \wfica32.exe"
                 }
 ,
```

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

```
41                  {
42
43                    "filePath": "C:\Program Files (x86)\Citrix\ICA Client
                         \AuthManager\AuthManSvr.exe"
44                   }
45
46                ]
47               }
48
49            ]
50           }
51
52        ]
53       }
54  ,
55     "name": "name",
56     "description": "desc",
57     "useForAppConfig": true
58    }
59
60  }
61
62 <!--NeedCopy-->
```

Configurar la detección de manipulación de directivas

March 11, 2024

Requisitos previos

Para configurar la función de detección de manipulación de directivas, asegúrese de tener lo siguiente:

- Para implementaciones en la nube: Cloud Desktop Delivery Controller, versión 115 o una posterior
- Para implementaciones locales: Citrix Virtual Apps and Desktops versión 2308 o una posterior
- Windows Virtual Delivery Agent Installer versión 2308 o una posterior
- Para Windows: Aplicación Citrix Workspace para Windows 2309 o una versión posterior
- Para Mac: Aplicación Citrix Workspace para Mac 2308 o una versión posterior
- Para Linux: Aplicación Citrix Workspace para Linux 2308 o una versión posterior

Para habilitar la detección de manipulación de directivas, el administrador debe iniciar **Citrix App-Protection Service** en los VDA de TS/WS que alojan las aplicaciones y escritorios virtuales configurados con App Protection.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

Realice uno de estos pasos para activar la detección de manipulación de directivas:

- Mediante el símbolo del sistema:

  1. En el extremo izquierdo de la barra de tareas, haga clic en el icono **Buscar** . Escriba **cmd** y, a continuación, haga clic en **Ejecutar como administrador**. Aparece la pantalla **Símbolo del sistema**.
  2. Ejecute los comandos siguientes:

```
sc config ctxappprotectionsvc start=auto
sc start ctxappprotectionsvc

<!--NeedCopy-->
```

- Con la interfaz de usuario:

  1. En el extremo izquierdo de la barra de tareas, haga clic en el icono **Buscar** . Escriba **services.msc** y presione **Entrar**. Aparece la pantalla **Servicios**.
  2. Seleccione **Citrix AppProtection Service** y, a continuación, haga clic en **Iniciar**.
  3. Haga clic con el botón secundario en **Citrix AppProtection Service** y, a continuación, seleccione **Propiedades**.
  4. Seleccione **General** > **Tipo de inicio** > **Automático** y, a continuación, haga clic en **Aceptar** para asegurarse de que el servicio se inicie automáticamente cuando se inicie el sistema.

La función de detección de manipulación de directivas se ha habilitado correctamente.

Para detectar y bloquear versiones anteriores de la aplicación Citrix Workspace que no admiten la detección de manipulaciones de directivas, configure la verificación de la postura de App Protection. Para obtener más información sobre la verificación de la postura de App Protection, consulte Verificación de la postura de App Protection.

Configurar la verificación de postura de App Protection

March 11, 2024

Para habilitar la verificación de la postura de App Protection, configure la nueva directiva de Citrix de VDA relacionada con esta función.

Requisitos previos

Asegúrese de tener lo siguiente:

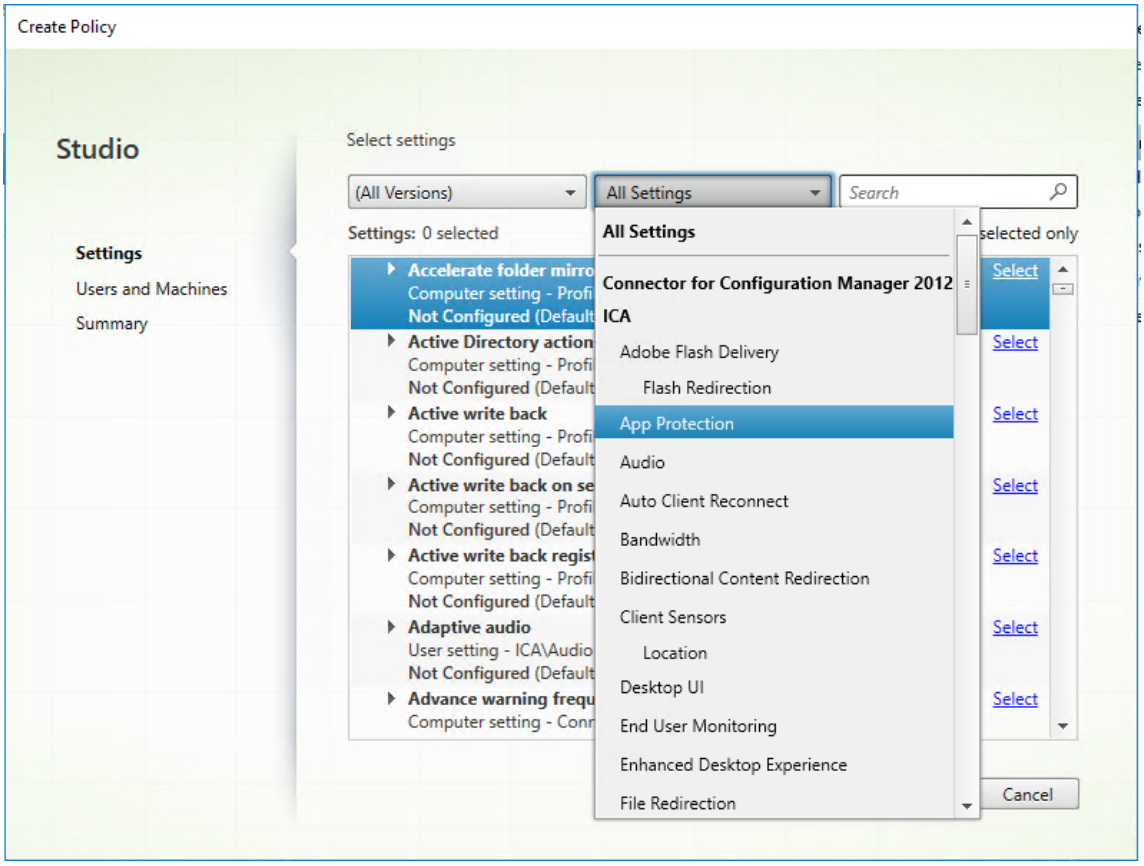
© 1999–2024 Cloud Software Group, Inc. All rights reserved.

- Para implementaciones en la nube: Cloud Desktop Delivery Controller, versión 115 o una posterior
- Para implementaciones locales: Citrix Virtual Apps and Desktops versión 2308 o una posterior
- Windows Virtual Delivery Agent Installer versión 2308 o una posterior
- Para Windows: Aplicación Citrix Workspace para Windows 2309 o una versión posterior
- Para Mac: Aplicación Citrix Workspace para Mac 2308 o una versión posterior
- Para Linux: Aplicación Citrix Workspace para Linux 2308 o una versión posterior

Configure la nueva directiva de Citrix de VDA para la comprobación de la postura de esta manera:

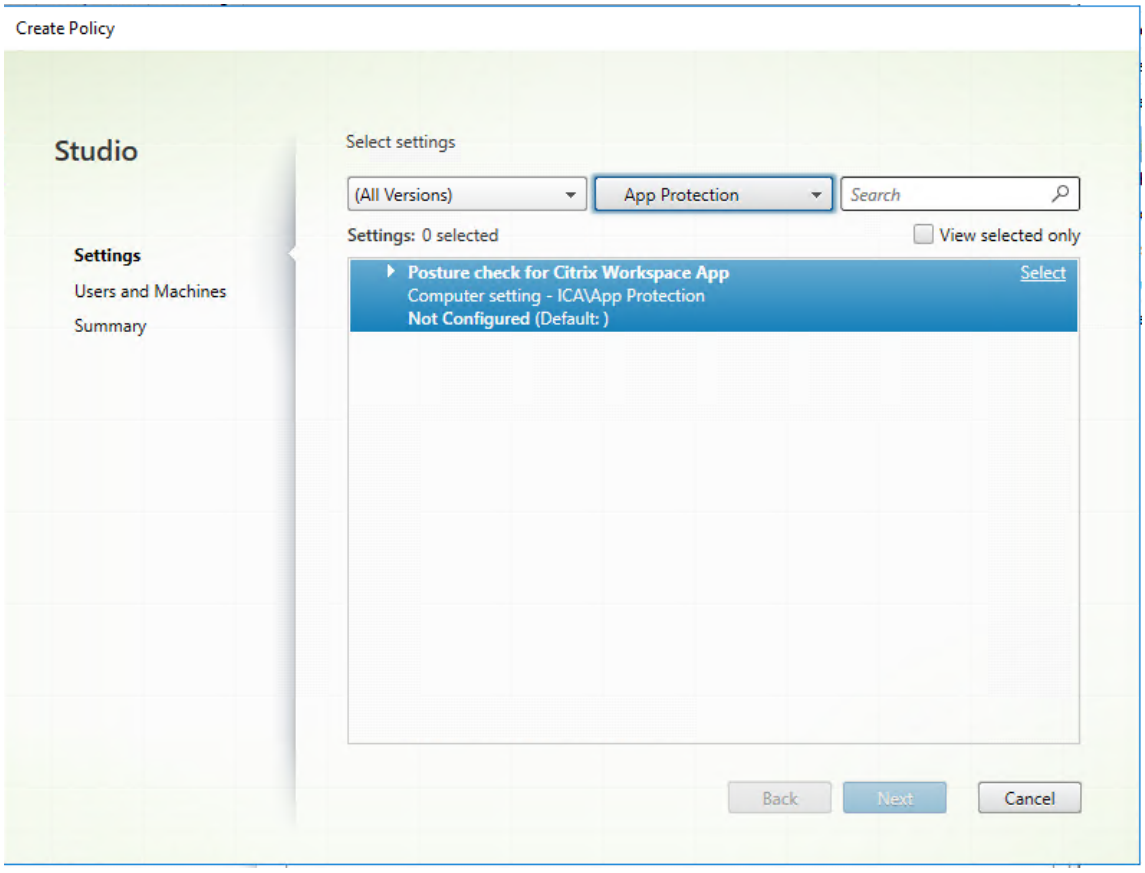
> **Nota:**
>
> Esta nueva directiva de Citrix de VDA se puede implementar mediante Citrix Studio y Web Studio. Este procedimiento se implementa a través de Citrix Studio. También puede utilizar el mismo procedimiento para Web Studio.

1. Abra la aplicación Citrix Studio en el Desktop Delivery Controller (DDC) para implementaciones locales o Web Studio para la nube y, a continuación, seleccione **Directivas**.
2. En **Acciones**, seleccione **Directivas** > **Crear directiva**.
3. Haga clic en el menú desplegable **Todos los parámetros** y seleccione **App Protection** en **ICA**.



© 1999–2024 Cloud Software Group, Inc. All rights reserved.

4. Seleccione **Comprobación de la postura para la aplicación Citrix Workspace** y después haga clic en **Seleccionar**.



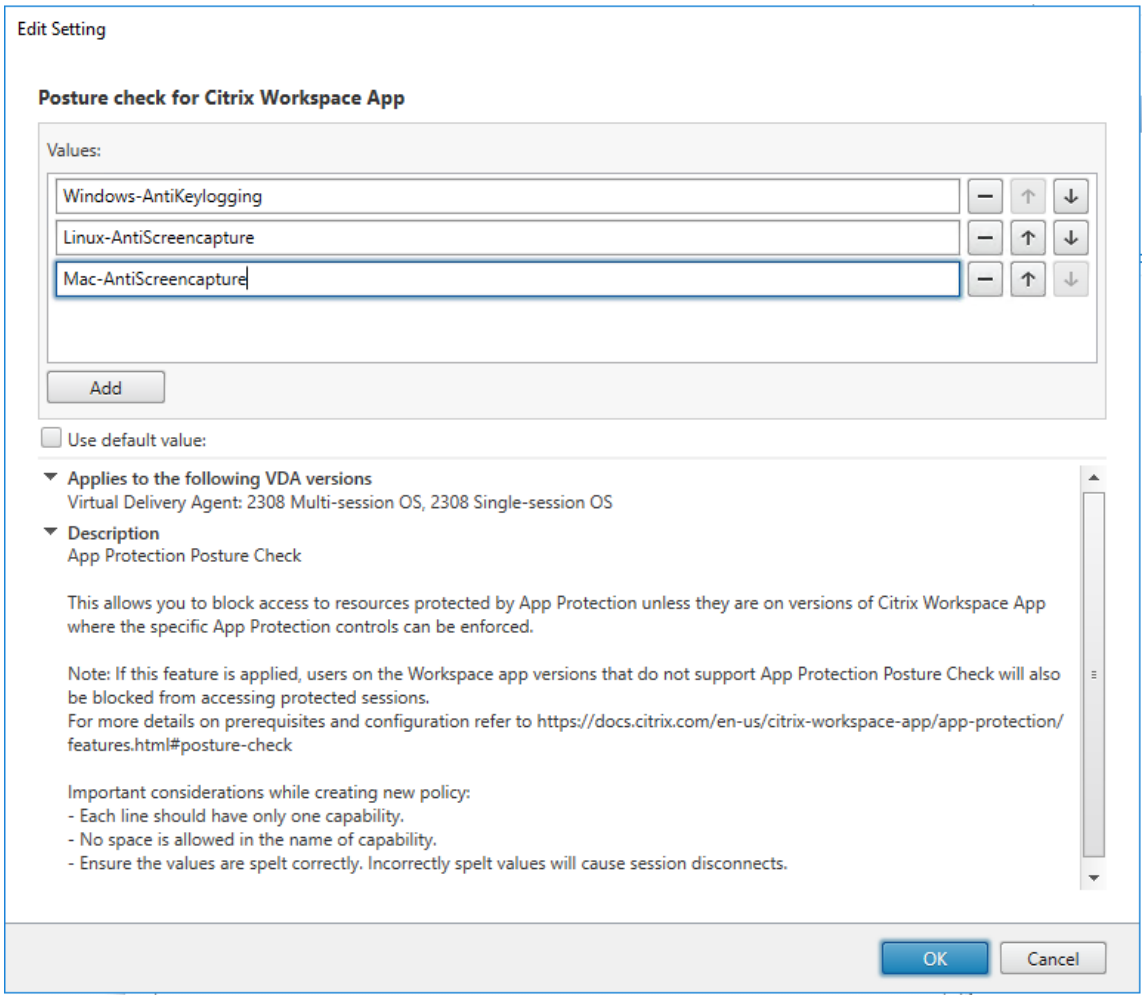
Se muestra la ventana **Modificar parámetro** .

5. Desactive la casilla de verificación **Usar valor predeterminado**.
6. Haga clic en **Agregar** e introduzca los valores correspondientes de entre los siguientes:

   - Windows-AntiScreencapture
   - Windows-AntiKeylogging
   - Linux-AntiScreencapture
   - Linux-AntiKeylogging
   - Mac-AntiScreencapture
   - Mac-AntiKeylogging

   Por ejemplo, si agregó “Windows-Protección contra capturas de pantalla”y “Windows-Protección contra registro de tecleo”, la aplicación Citrix Workspace para Windows que tiene disponible la función Comprobación de la postura y tiene estas prestaciones puede conectarse al VDA.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

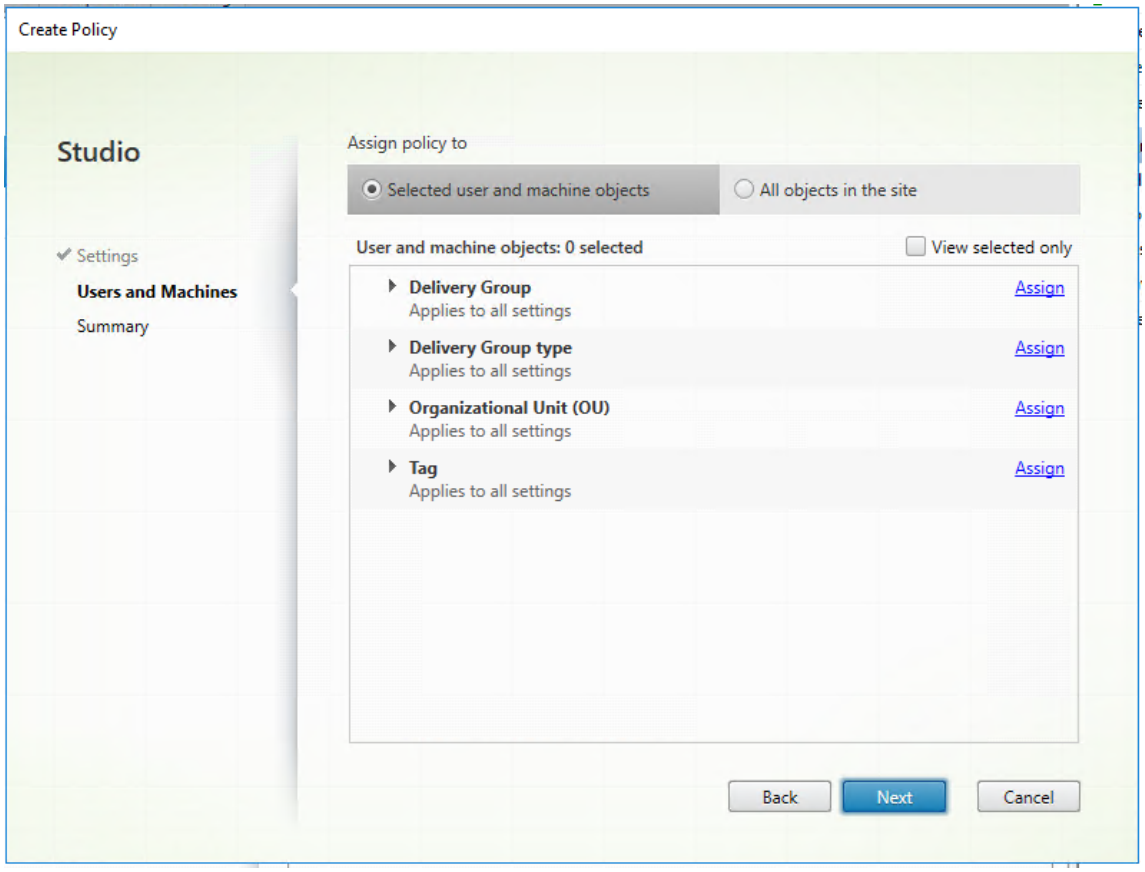


Nota:

- Cada entrada debe tener solo una prestación.
- No se permiten espacios en el nombre de la prestación.
- Asegúrese de que los valores estén escritos correctamente. Los valores mal escritos harán que la sesión se cierre.
- Se ignoran los valores que no tengan los prefijos Windows-, Linux- o Mac-.

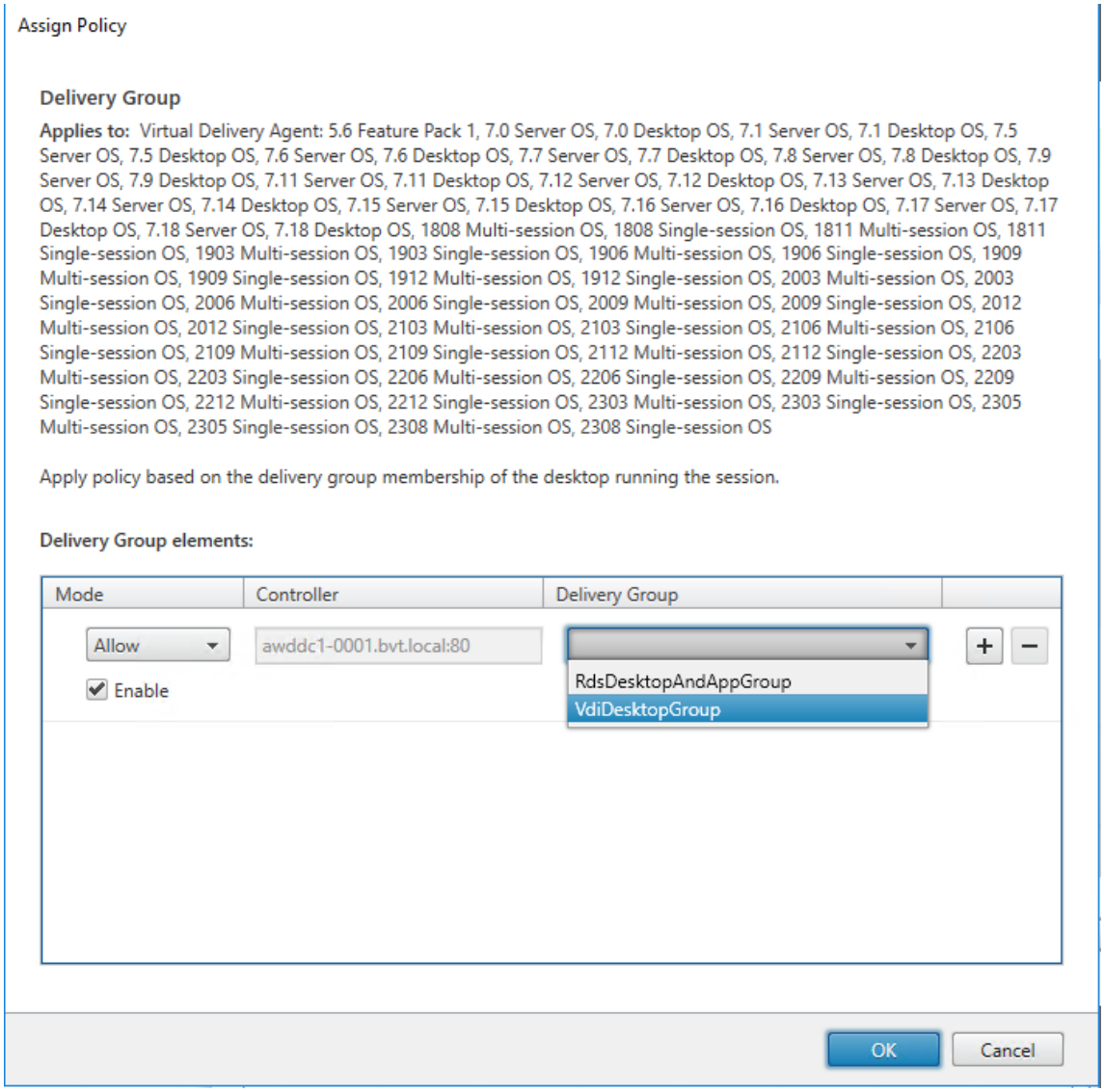
7. Tras agregar todos los valores necesarios, haga clic en **Aceptar**.
8. Haga clic en **Siguiente**.
9. Seleccione **Asignar directiva a** > **Usuarios y objetos de máquina seleccionados**.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.



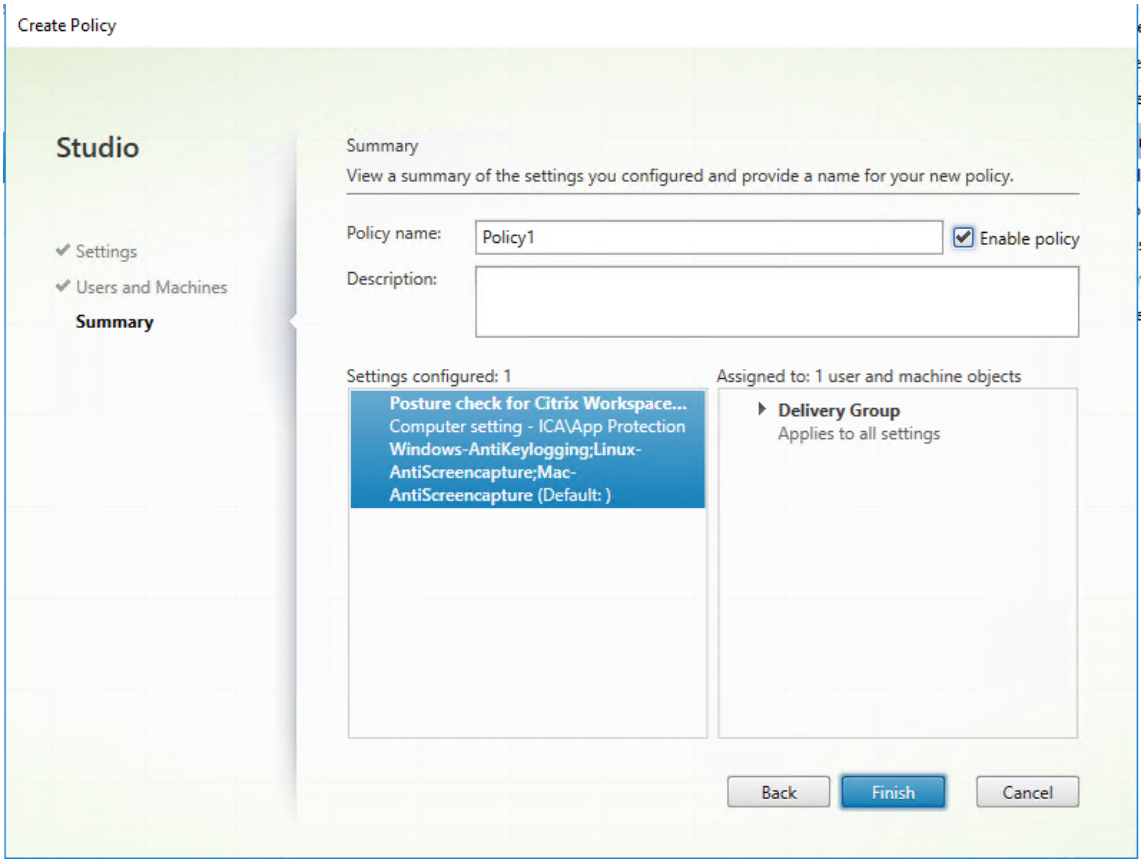
10. Seleccione los grupos de entrega necesarios en los que debe implementarse esta directiva y, a continuación, haga clic en **Aceptar**.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.



11. Haga clic en **Siguiente**.
12. Introduzca el nombre de la directiva en el campo **Nombre de la directiva** y, a continuación, marque la casilla **Habilitar directiva**.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.



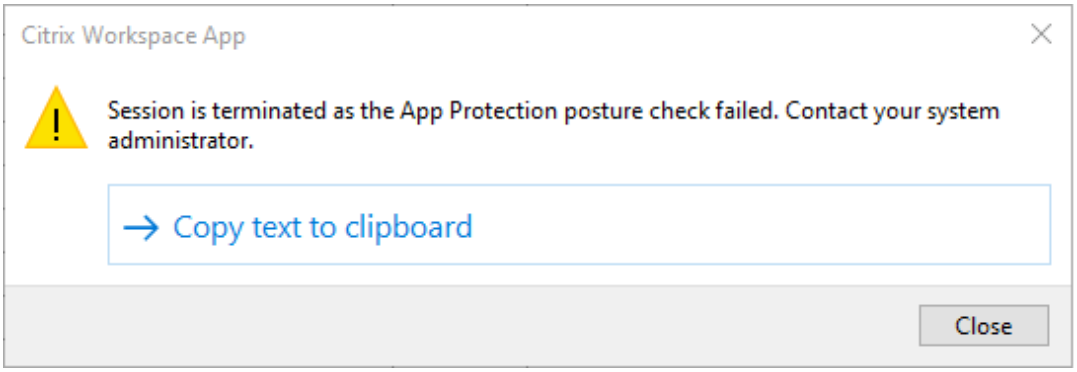
13. Haga clic en **Finalizar**.

Se crea una directiva para la comprobación de la postura.

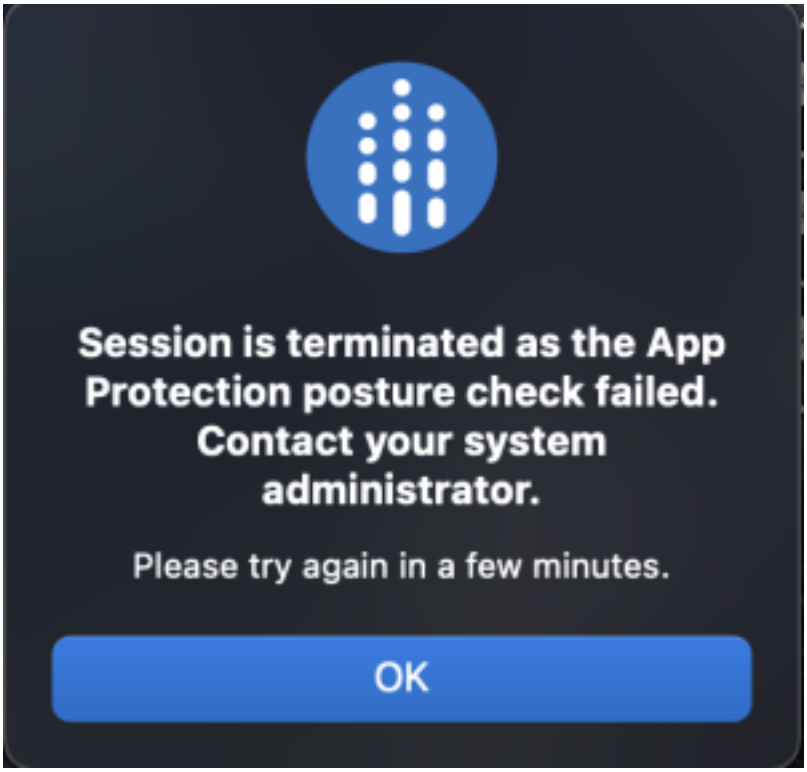
Comportamiento esperado si se produce un error en la Comprobación de la postura de App Protection

- Si la directiva de Citrix de VDA de Comprobación de la postura está habilitada y está usando una versión de la aplicación Citrix Workspace que no tiene disponible la función de Comprobación de la postura, la sesión finaliza sin mostrar ningún mensaje de error.
- Si usa una versión de la aplicación Citrix Workspace que dispone de la función de Comprobación de la postura, la sesión finaliza y muestra estos mensajes de error, respectivamente:
  - Windows:

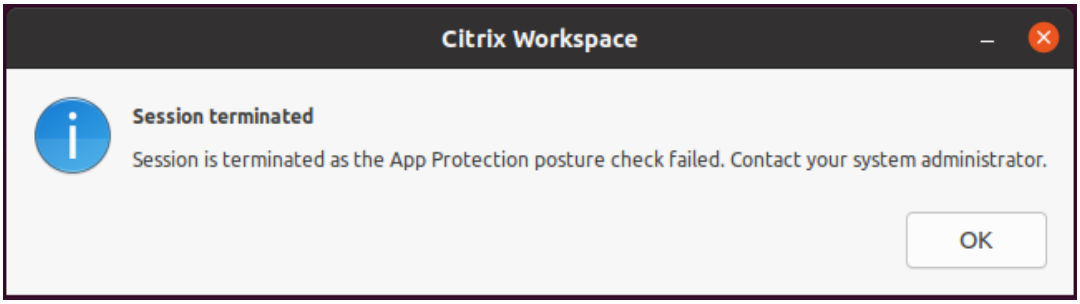
© 1999–2024 Cloud Software Group, Inc. All rights reserved.



- Mac



- Linux



© 1999–2024 Cloud Software Group, Inc. All rights reserved.

Bloquear inicio de doble salto

March 11, 2024

Para bloquear el inicio del doble salto, asegúrese de ejecutar la aplicación Citrix Workspace para Windows 2309 o una versión posterior en el primer salto.

Implemente las siguientes configuraciones en todos los VDA en el primer salto:

1. Actualice las directivas de GPO más recientes. Para obtener más información, consulte Actualizar las directivas de GPO más recientes.
2. Inicie el **Editor de directivas de grupo** y, a continuación, vaya a **Configuración del equipo** > **Plantillas administrativas** > **Componentes de Citrix** > **Citrix Workspace** > **App Protection** > **Bloquear inicio de doble salto**.
3. Seleccione **Habilitada** y haga clic en **Aceptar**.

   El parámetro **Bloquear inicio de doble salto** está habilitado y no podrá realizar inicios de doble salto.

> **Nota:**
>
> El sistema operativo Windows Server no admite App Protection. Por lo tanto, las instancias de Virtual Apps and Desktops que están habilitadas con App Protection no se muestran si está ejecutando un sistema operativo de servidor Windows en el primer salto.

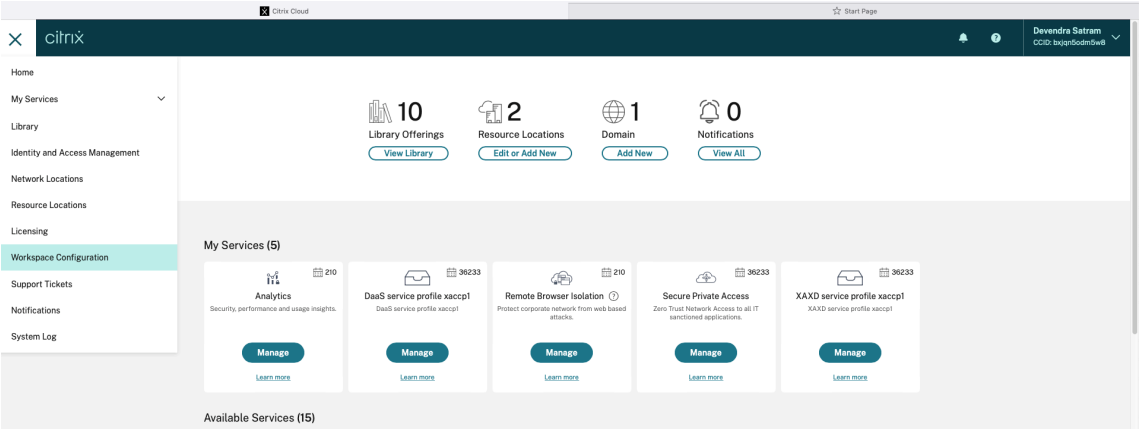
Configurar Lista de permitidos para capturas de pantalla

April 25, 2024

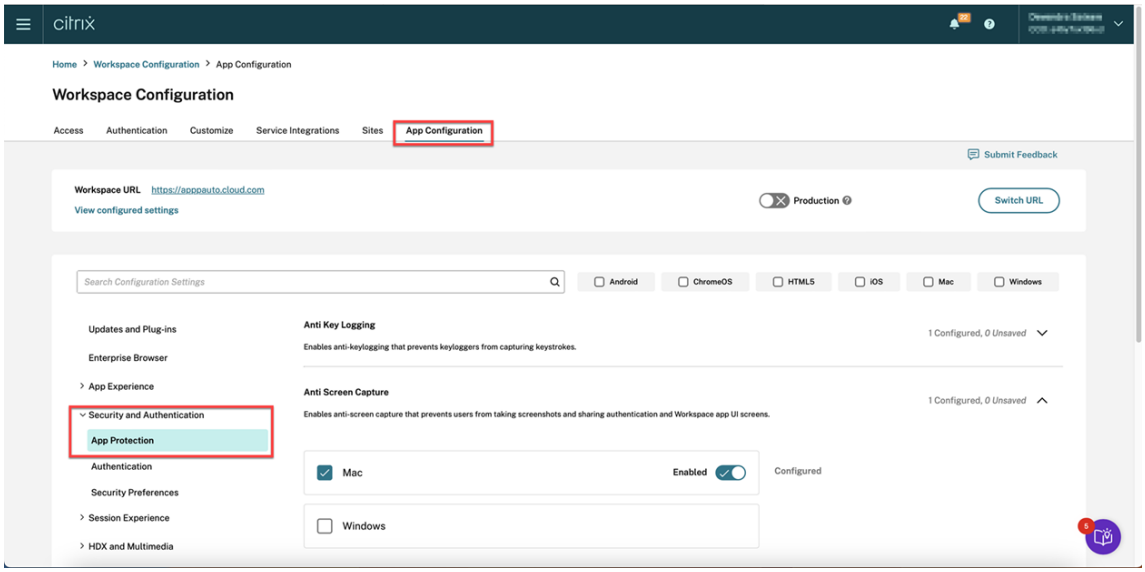
Para agregar una aplicación a la lista de permitidos para capturas de pantalla, siga estos pasos:

1. Inicie sesión en su cuenta de Citrix Cloud y seleccione **Configuración de Workspace**.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

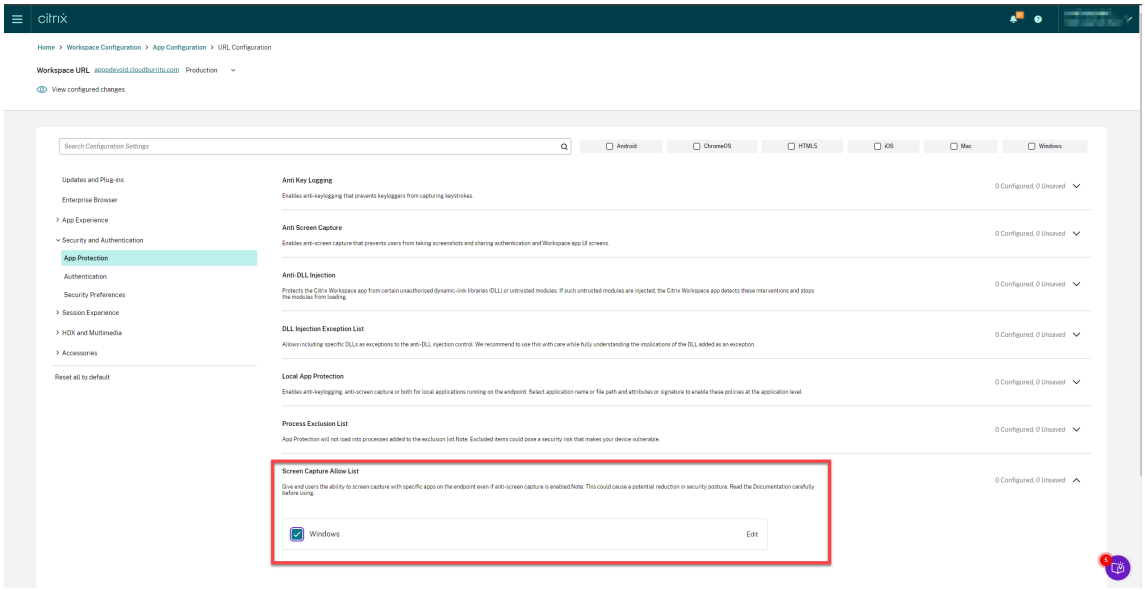


2. Seleccione **Configuración de la aplicación** > **Seguridad y autenticación** > **Configurar** > **App Protection**.



3. Haga clic en **Lista de permitidos para capturas de pantalla** y seleccione la casilla de verificación de **Windows**.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.



4. Haga clic en la opción **Modificar**.

   Aparecerá la pantalla **Administrar parámetros de Windows**.

5. Agregue la información sobre la aplicación que quiere agregar a la Lista de permitidos para capturas de pantalla.

   Por ejemplo:

```
[
 {

 "name": "ScreenshotTool_1.exe",
 "signature": "ScreenshotTool_1 Signature",
 "publisher": "ScreenshotTool_1 Publisher"
  }
 ,
 {

  "name": "Screenshottool_2.exe",
  "signature": "",
  "publisher": ""
  }

]
<!--NeedCopy-->
```

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

Manage settings for Windows

```
[
  {
    "name": "ScreenshotTool_1.exe",
    "signature": "ScreenshotTool_1_Signature",
    "publisher": "ScreenshotTool_1_Publisher"
  },
  {
    "name": "ScreenshotTool_2.exe",
    "signature": "",
    "publisher": ""
  }
]
```

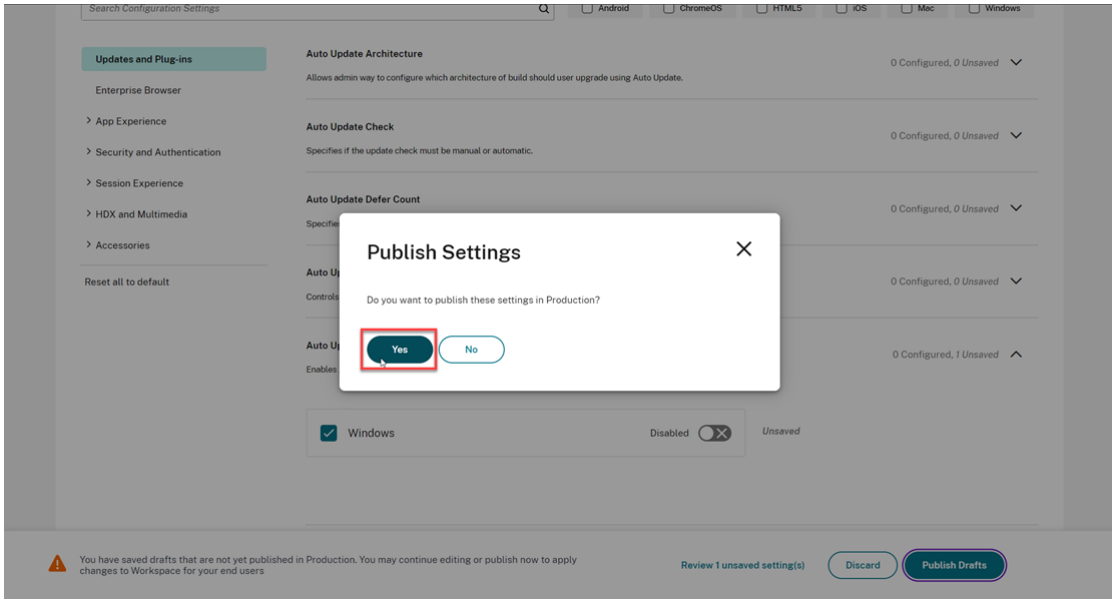
Save draft Cancel

> **Nota:**
>
> - `name` debe rellenarse obligatoriamente. Al mismo tiempo, `publisher` y `signature` no son obligatorios. Sin embargo, se recomienda agregar los valores `publisher` y `signature` correspondientes para asegurarse de que solo la aplicación de la lista de permitidos pueda realizar las capturas de pantalla.
> - Sin los valores de valores `publisher` y `signature`, una aplicación maliciosa con el mismo nombre puede realizar capturas de pantalla.
> - Además, puede agregar varias aplicaciones a la lista de permitidos para capturas de pantalla agregando varias entradas en este bloque.

Para obtener la información de `publisher` y `signature`, consulte Obtener la información de `publisher` y `signature`.

6. Haz clic en **Guardar borrador** y, a continuación, en **Publicar borradores**.
7. En el cuadro de diálogo **Parámetros de publicación**, haga clic en **Sí**.

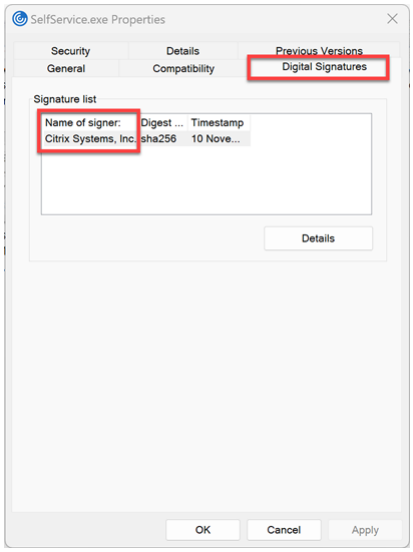
© 1999–2024 Cloud Software Group, Inc. All rights reserved.



Obtener la información de `publisher` y `signature`

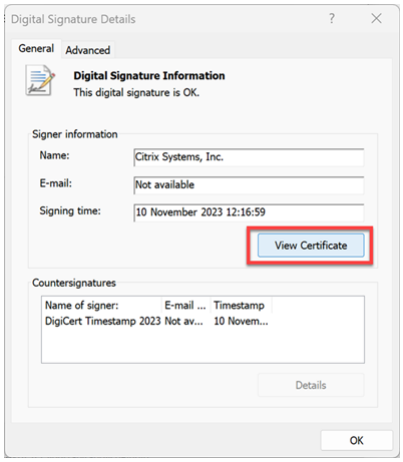
Para obtener la información de `publisher` y `signature`, siga estos pasos:

1. Abra la ubicación del archivo donde tiene el archivo `.exe` de la aplicación correspondiente.
2. Haga clic con el botón secundario en el archivo `.exe` y, a continuación, en **Propiedades**. Aparece una pantalla emergente de propiedades.
3. Haga clic en **Firmas digitales**. El **nombre del firmante** es el valor de `publisher`.

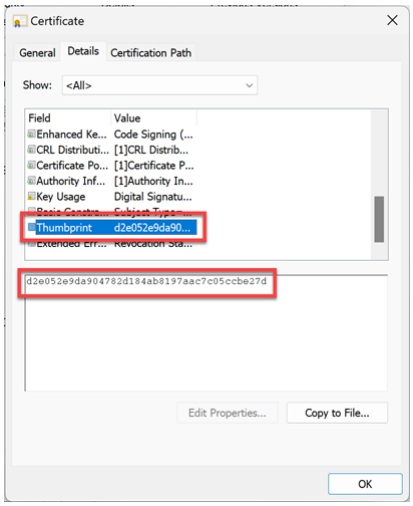


4. Haga clic en la primera entrada del **nombre del firmante** y, a continuación, haga clic en **Detalles** > **Ver certificado**.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.



5. Haga clic en **Detalles** > **Huella digital**. El contenido que aparece en el cuadro de texto es la `signature`.



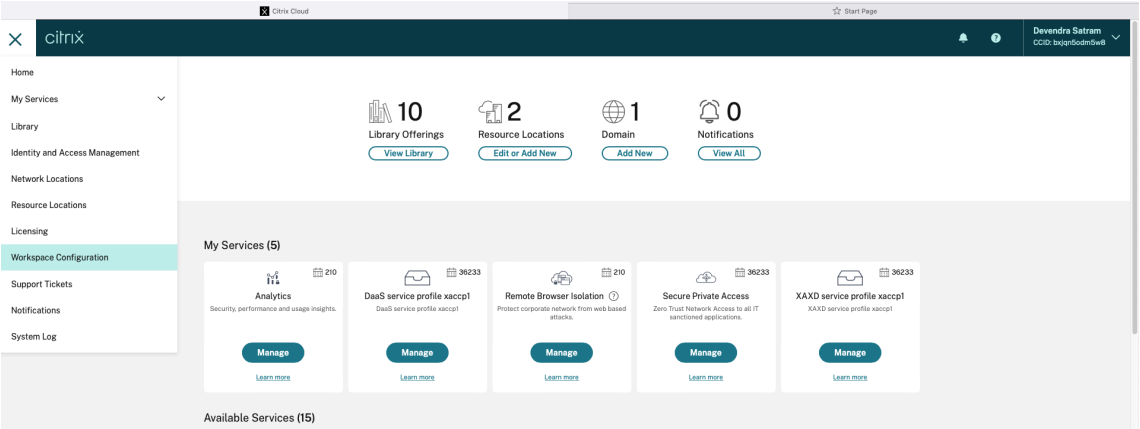
Configurar Lista de exclusión de procesos

April 25, 2024

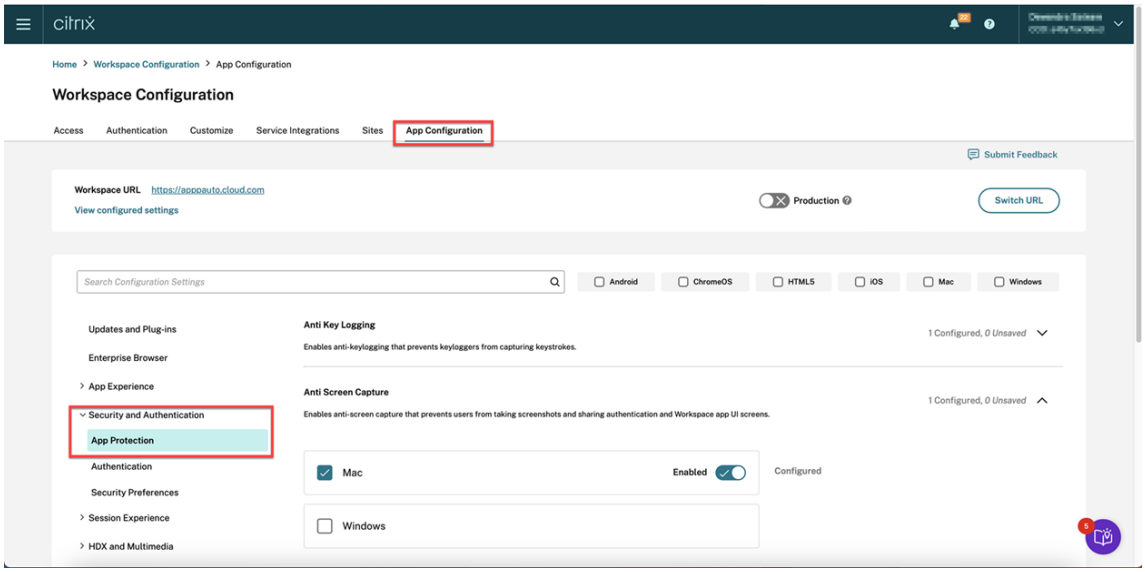
Para agregar un proceso a la Lista de exclusiones de procesos, siga estos pasos:

1. Inicie sesión en su cuenta de Citrix Cloud y seleccione **Configuración de Workspace**.

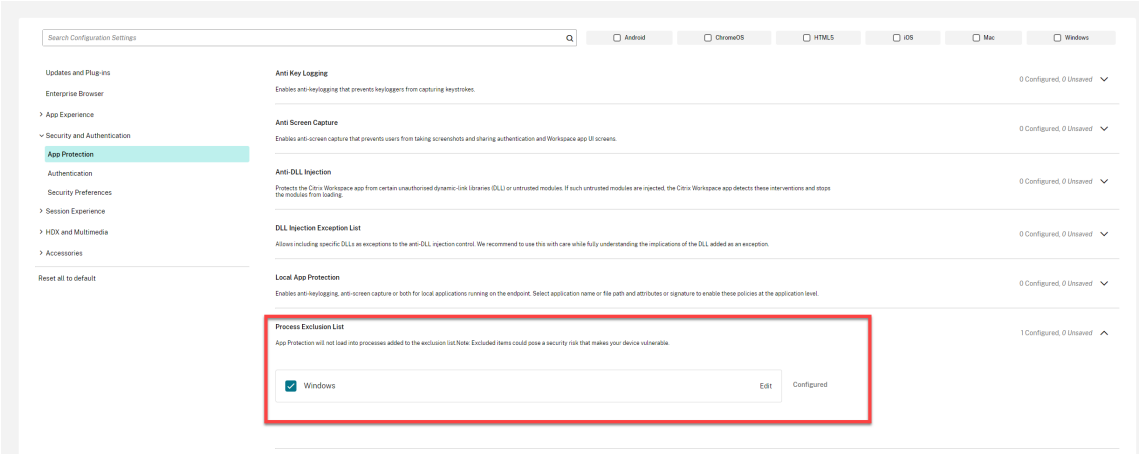
© 1999–2024 Cloud Software Group, Inc. All rights reserved.



2. Seleccione **Configuración de la aplicación** > **Seguridad y autenticación** > **Configurar** > **App Protection**.



3. Haga clic en **Lista de exclusión de procesos** y, a continuación, seleccione la casilla de verificación de **Windows**.



© 1999–2024 Cloud Software Group, Inc. All rights reserved.

4. Haga clic en la opción **Modificar**.

   Aparecerá la pantalla **Administrar parámetros de Windows**.

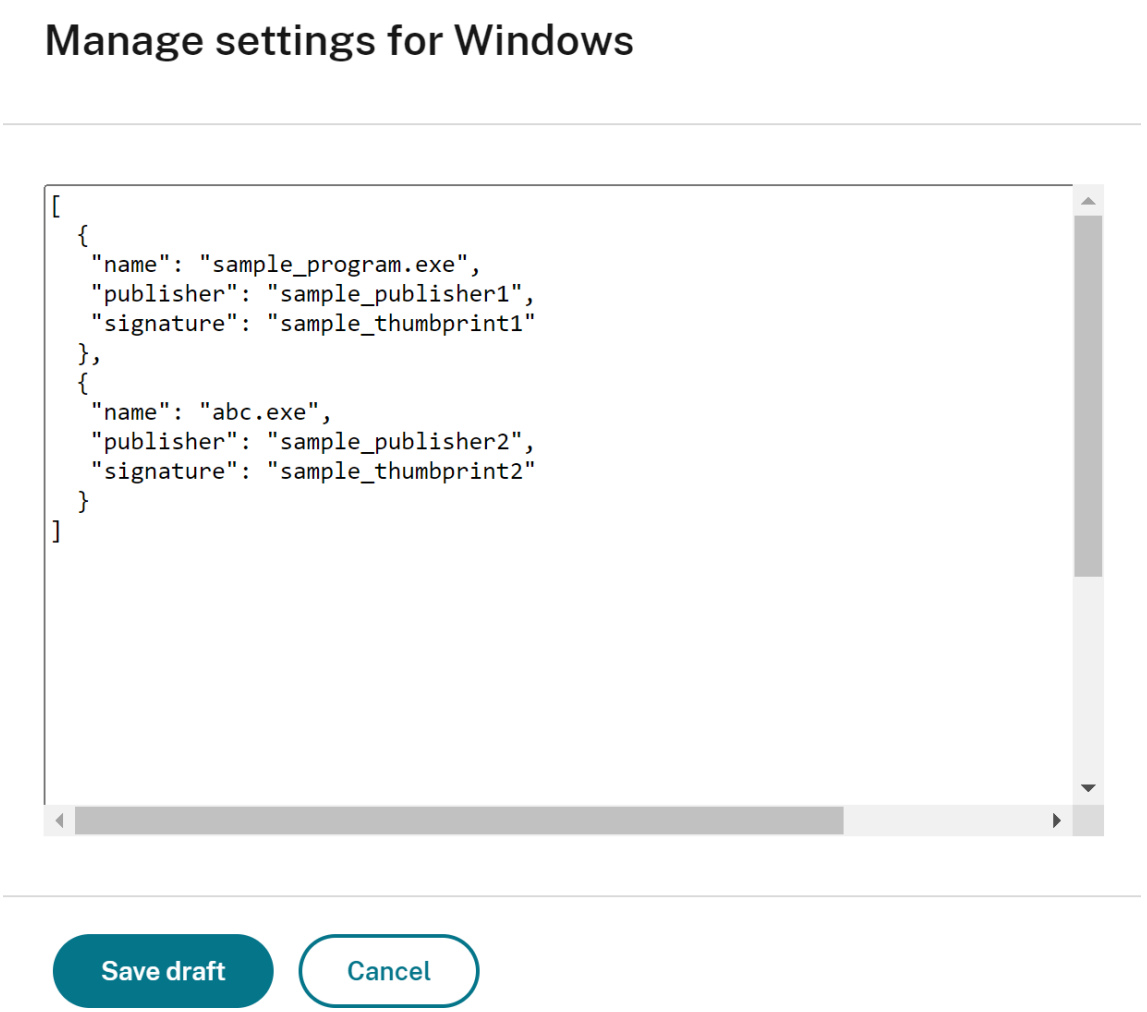
5. Agregue la información sobre el proceso que quiere agregar a la Lista de exclusión de procesos.

   Por ejemplo:

```
[
 {

  "name": "sample_program.exe",
  "publisher": "sample_publisher1",
  "signature": "sample_thumbprint1"
  }

]
<!--NeedCopy-->
```

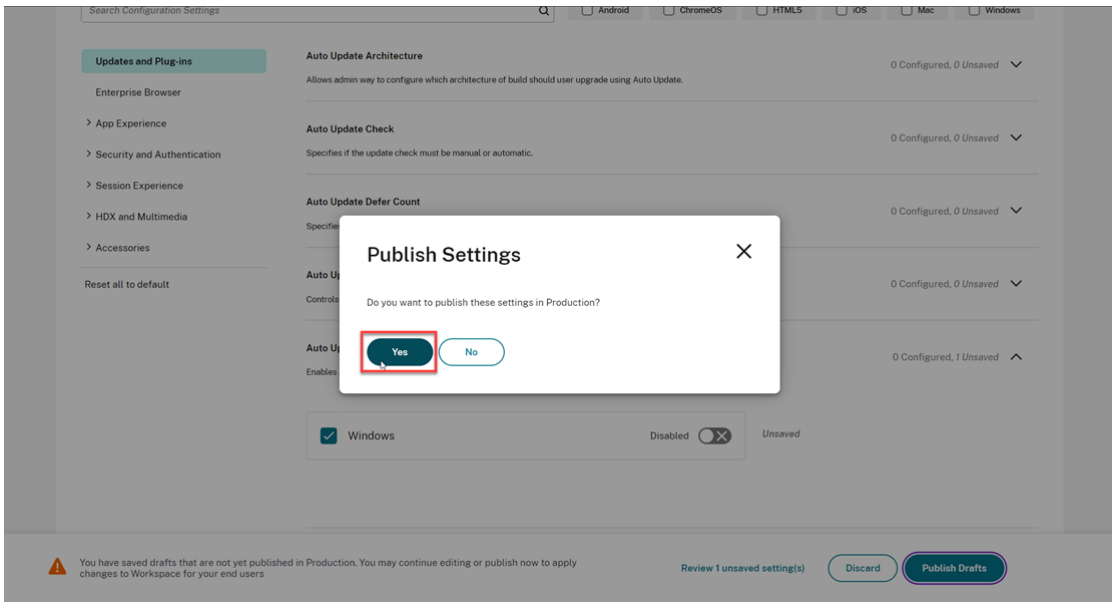


© 1999–2024 Cloud Software Group, Inc. All rights reserved.

> **Nota:**
>
> - `name` debe rellenarse obligatoriamente. Al mismo tiempo, `publisher` y `signature` no son obligatorios. Sin embargo, se recomienda agregar `publisher` y `signature` para asegurarse de que se agrega el proceso correcto a la lista.
> - Además, puede agregar varios procesos a la Lista de exclusión de procesos agregando varias entradas en este bloque.

Para obtener la información de `publisher` y `signature`, consulte Obtener la información de `publisher` y `signature`.

6. Haz clic en **Guardar borrador** y, a continuación, en **Publicar borradores**.
7. En el cuadro de diálogo **Parámetros de publicación**, haga clic en **Sí**.



8. Reinicie la aplicación Citrix Workspace.

Configurar Lista de exclusión de controladores de filtro USB

April 25, 2024

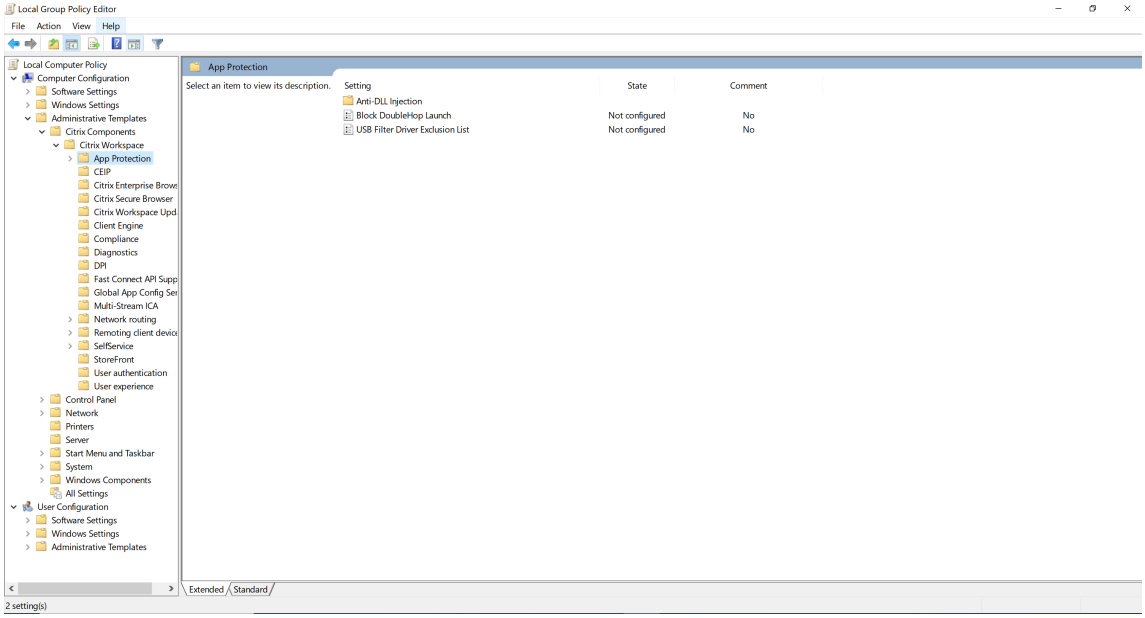
Puede agregar un dispositivo USB a la Lista de exclusión de controladores de filtro USB mediante uno de los métodos siguientes:

- Mediante un objeto de directiva de grupo
- Mediante la interfaz de usuario de Global App Configuration Service

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

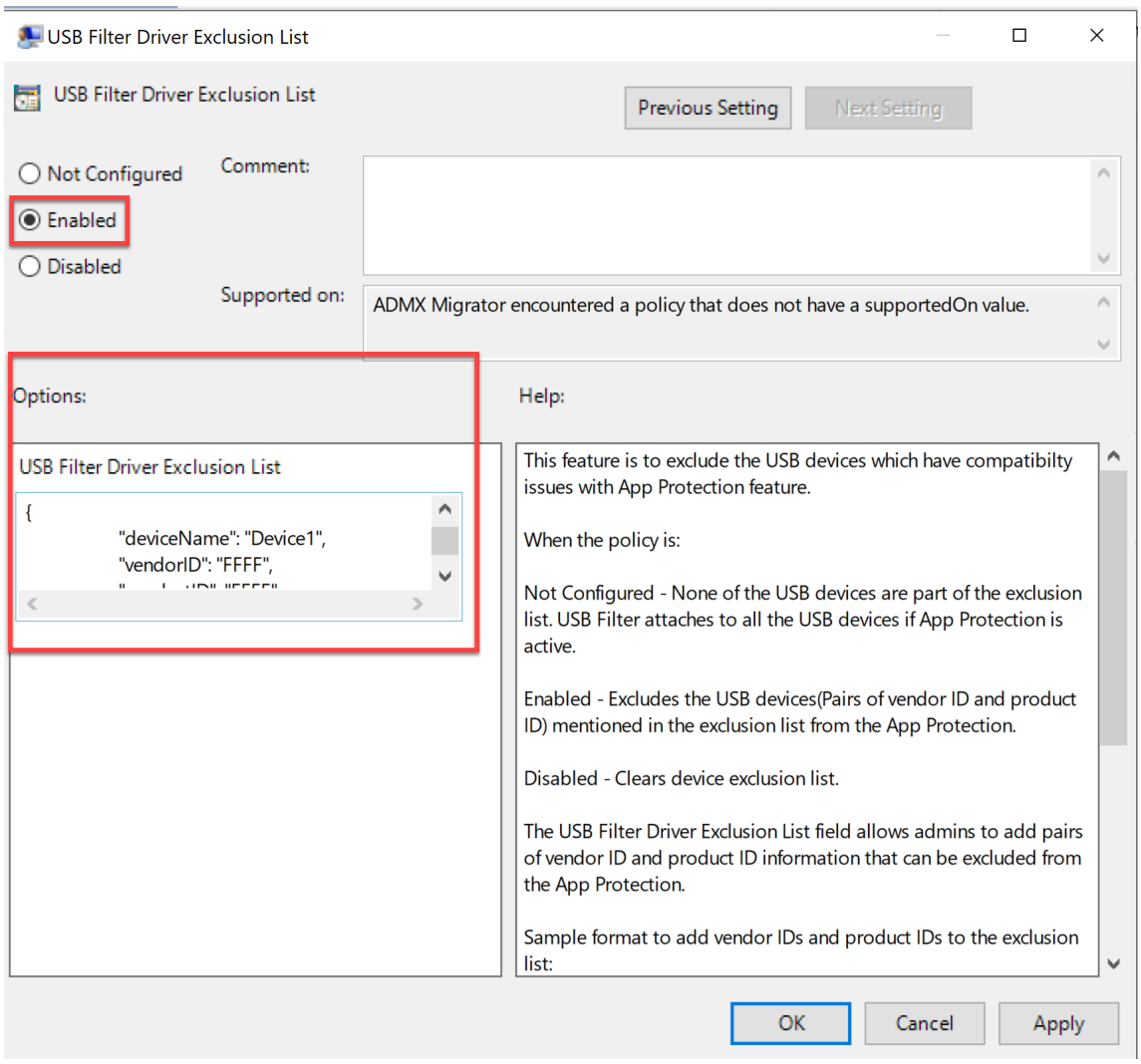
Mediante un objeto de directiva de grupo

1. Abra la plantilla administrativa de GPO de la aplicación Citrix Workspace; para ello, ejecute `gpedit.msc`. Para obtener más información, consulte Objeto de directiva de grupo.
2. En el nodo **Configuración del equipo**, vaya a **Plantillas administrativas** > **Componentes de Citrix** > **Citrix Workspace** > **App Protection** > **Lista de exclusión de controladores de filtro USB**.



3. Seleccione **Habilitado** e introduzca el **ID de proveedor** y el **ID de producto** del dispositivo USB que quiere excluir en el cuadro de texto **Opciones**.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.



> **Nota:**
>
> - `productID` y `vendorID` deben rellenarse obligatoriamente. Al mismo tiempo, `deviceName` no es obligatorio.
> - Además, puede agregar varios dispositivos USB a la lista de exclusión agregando varias entradas en este bloque.

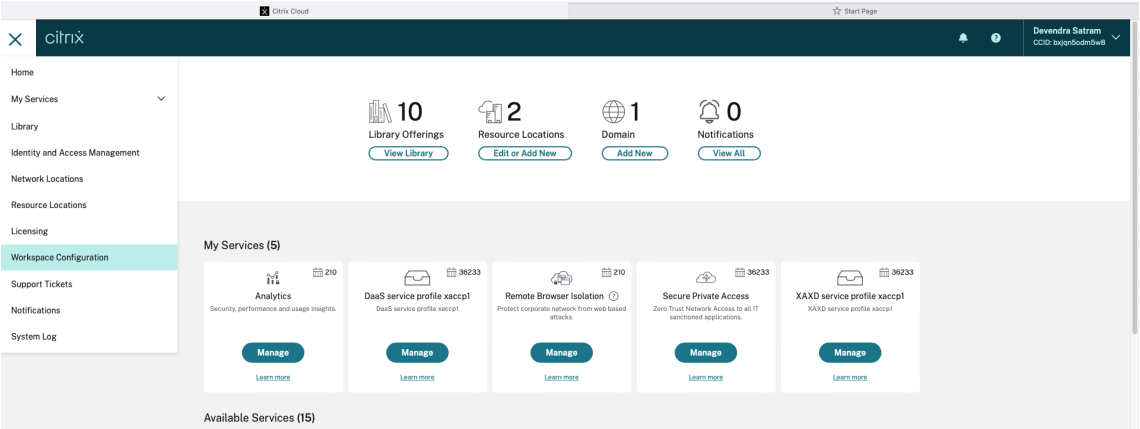
Para obtener `productID` y `vendorID`, consulte Obtener `productID` y `vendorID`.

4. Haga clic en **Aceptar**.

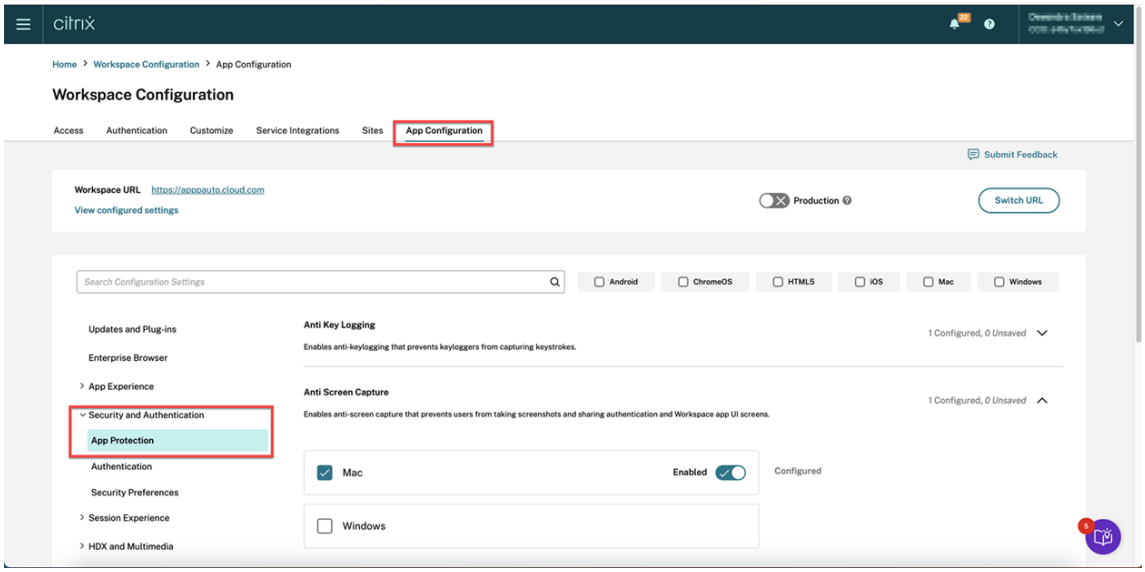
Mediante la interfaz de usuario de Global App Configuration Service

1. Inicie sesión en su cuenta de Citrix Cloud y seleccione **Configuración de Workspace**.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

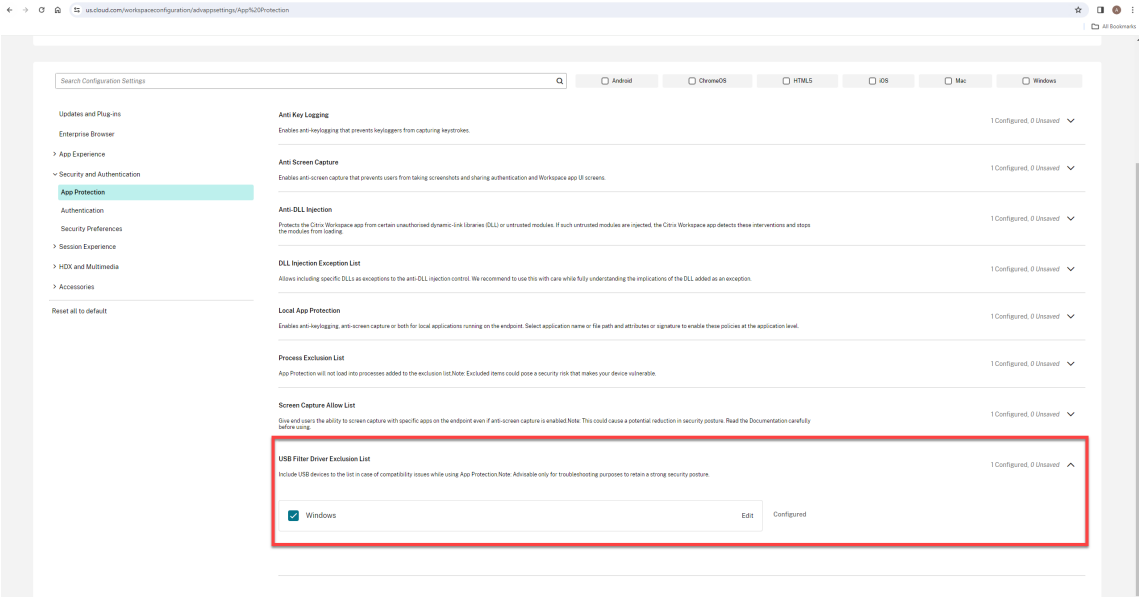


2. Seleccione **Configuración de la aplicación** > **Seguridad y autenticación** > **Configurar** > **App Protection**.



3. Haga clic en **Lista de exclusión de controladores de filtro USB** y, a continuación, seleccione la casilla de verificación de **Windows**.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.



4. Haga clic en la opción **Modificar**.

   Aparecerá la pantalla **Administrar parámetros de Windows**.

5. Agregue la información sobre el proceso o la aplicación que quiere agregar a la Lista de exclusión de controladores de filtro USB.

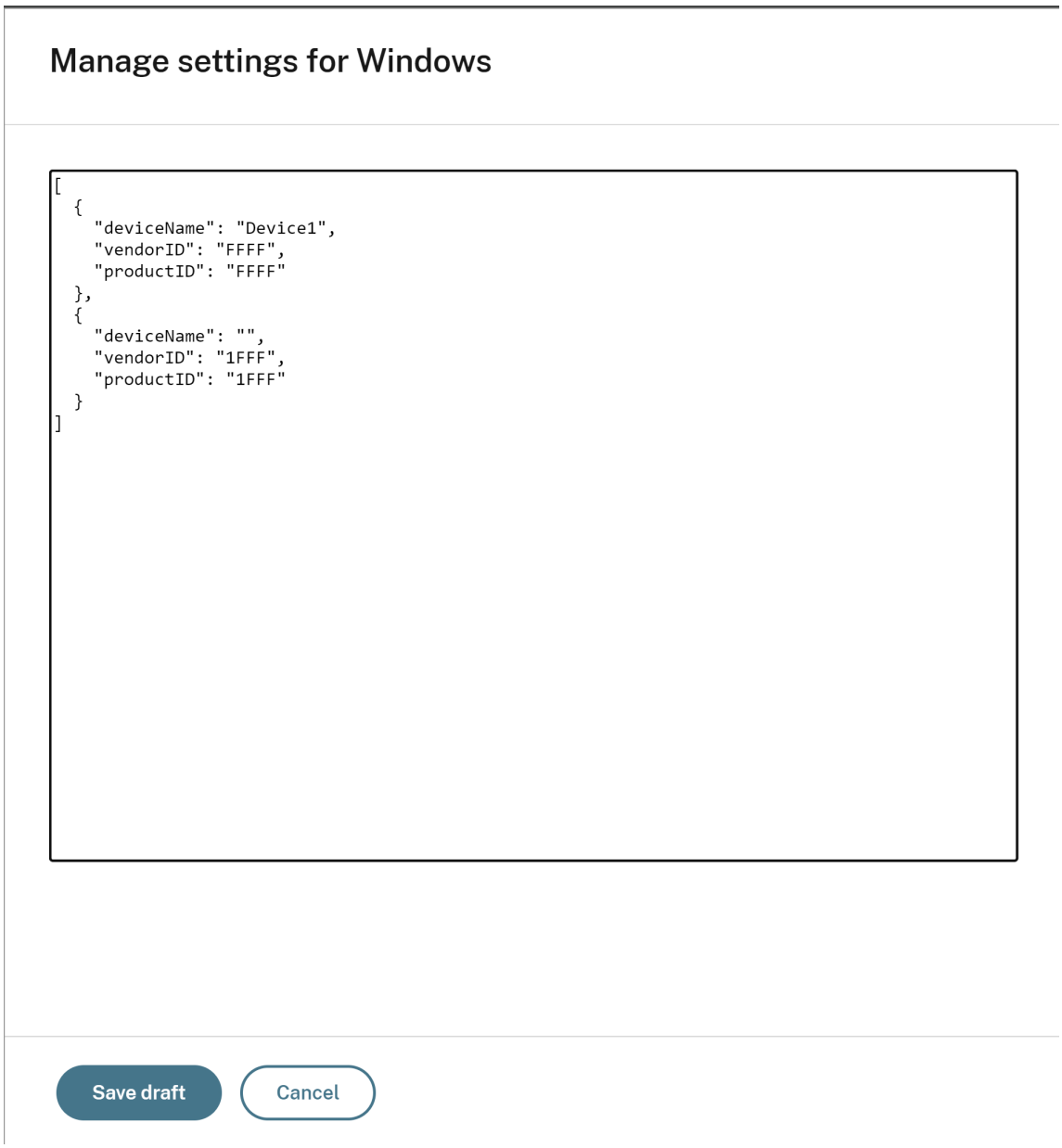
   Por ejemplo:

```
[
 {

  "deviceName": "Device1",
  "vendorID": "FFFF",
  "productID": "FFFF"
  }

]
<!--NeedCopy-->
```

© 1999–2024 Cloud Software Group, Inc. All rights reserved.



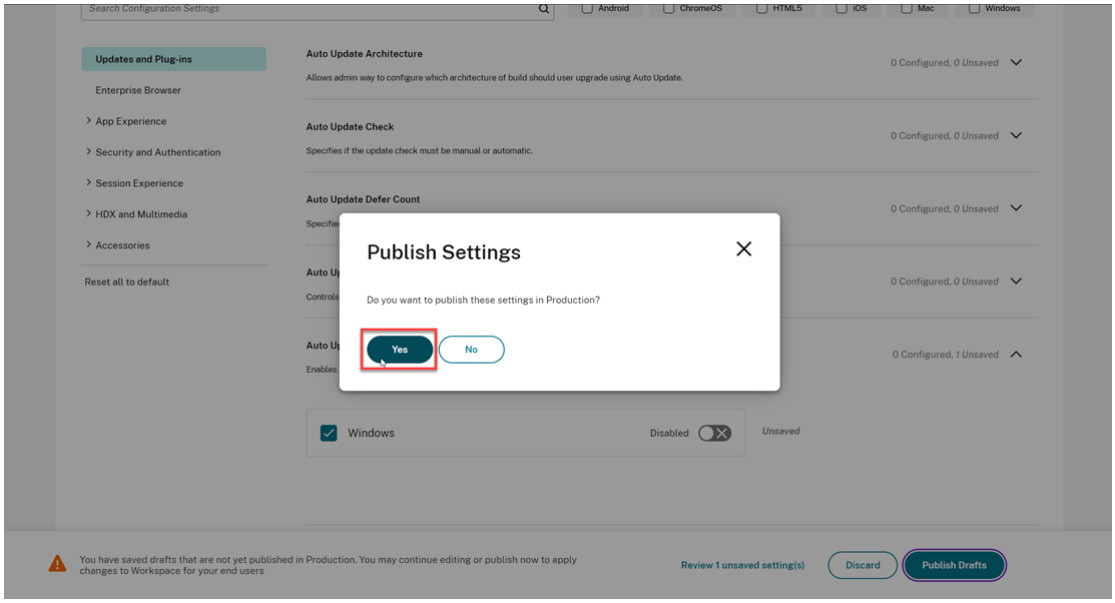
Nota:

- `productID` y `vendorID` deben rellenarse obligatoriamente. Al mismo tiempo, `deviceName` no es obligatorio.
- Además, puede agregar varios dispositivos USB a la lista de exclusión agregando varias entradas en este bloque.

Para obtener `productID` y `vendorID`, consulte Obtener `productID` y `vendorID`.

6. Haz clic en **Guardar borrador** y, a continuación, en **Publicar borradores**.
7. En el cuadro de diálogo **Parámetros de publicación**, haga clic en **Sí**.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.



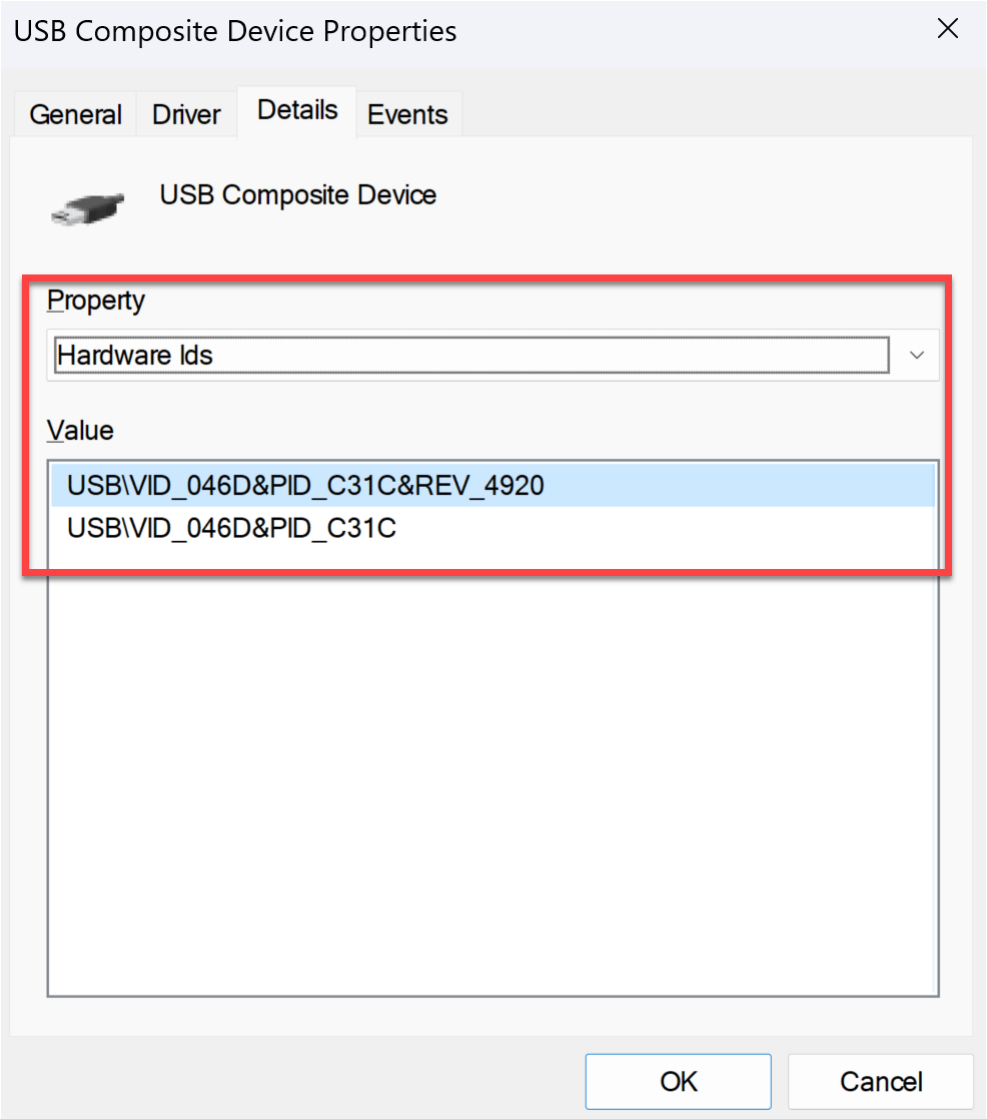
8. Reinicie la aplicación Citrix Workspace.

Obtener `productID` y `vendorID`

Para obtener `productID` y `vendorID`, siga estos pasos:

1. Abra el **Administrador de dispositivos** y busque el dispositivo que quiere agregar a la lista de exclusión.
2. Haga clic con el botón secundario en el nombre del dispositivo y, a continuación, en **Propiedades**. Aparece una pantalla emergente de propiedades.
3. Haga clic en **Detalles** y, a continuación, seleccione la opción **ID de hardware** en la lista de **propiedades**.
4. En el campo **Valor**, el valor con el prefijo `VID_` es el `vendorID` y el valor con el prefijo `PID_` es el `productID`.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.



Solucionar problemas técnicos

March 11, 2024

En este artículo se explica cómo solucionar problemas de App Protection en diferentes plataformas para la aplicación Citrix Workspace.

Para ver distintos casos de solución de problemas, consulte lo siguiente:

- Casos de solución de problemas genéricos
- Detección de manipulación de directivas
- Verificación de postura de App Protection

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

Aplicación Citrix Workspace para Windows

1. Recopilar registros como se describe en la recopilación de registros.
2. Presione **Win + R** para abrir el cuadro Ejecutar > escriba `cmd` > presione **Entrar**.
3. Ejecute los comandos siguientes:
   - Si usa una versión de la aplicación Citrix Workspace para Windows anterior a la 2311, ejecute los siguientes comandos:
     - `sc query appprotectionsvc`
     - `sc query entryprotectdrv`
     - `sc query epinject6`
     - `sc query epusbfilter`
   - Si usa la versión 2311 o posterior de la aplicación Citrix Workspace para Windows, ejecute los siguientes comandos:
     - `sc query appprotectionsvc`
     - `sc query ctxapdriver`
     - `sc query ctxapinject`
     - `sc query ctxapusbfilter`

Proporcione los resultados junto con los rastros recopilados en la herramienta de recopilación de registros.

Aplicación Citrix Workspace para Mac

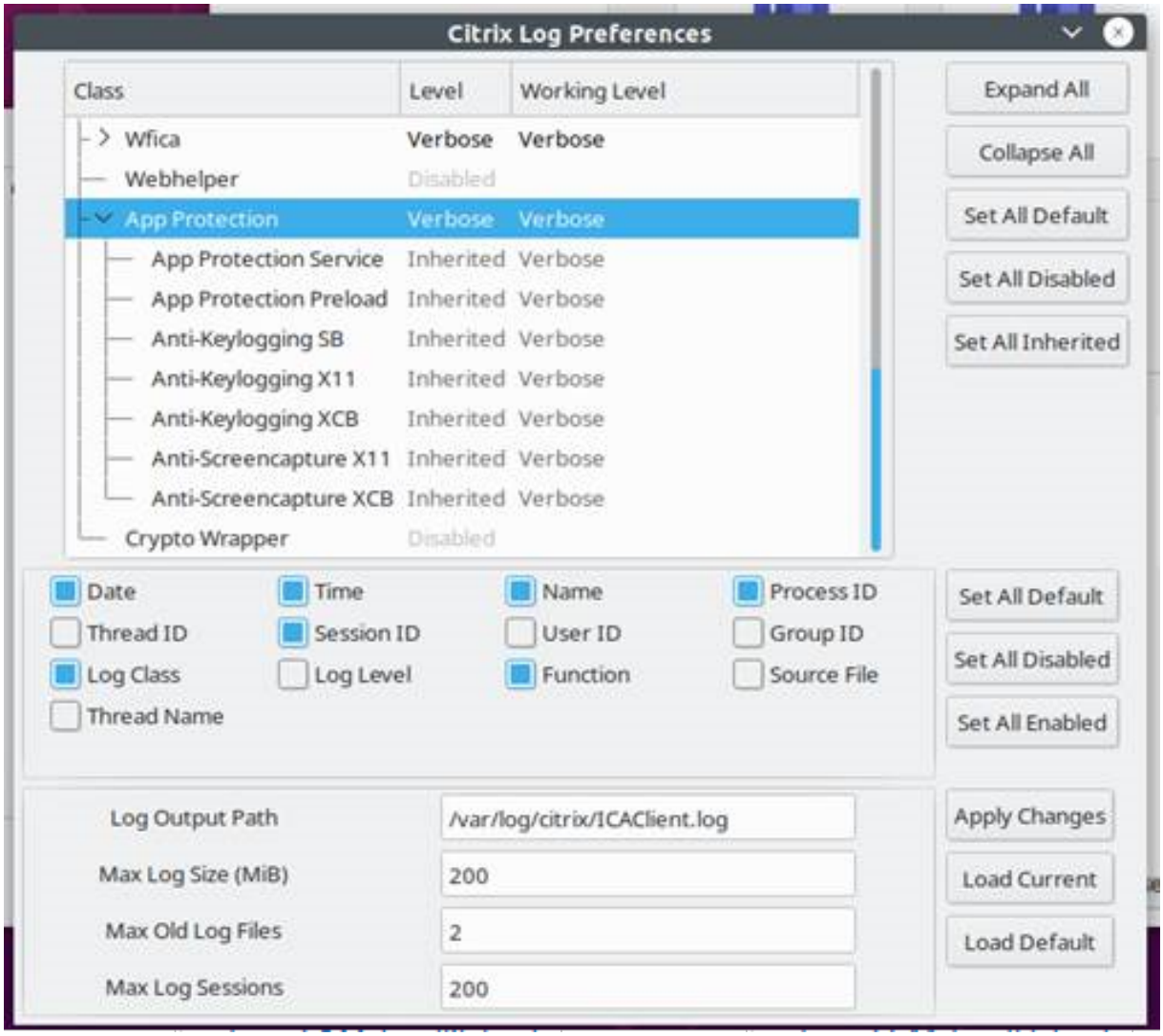
Proporcione los registros tras recopilarlos como se describe en la recopilación de registros.

Aplicación Citrix Workspace para Linux

1. Ejecute el ejecutable set log que se encuentra en la carpeta *util* de la instalación. Por ejemplo: `/opt/Citrix/ICAClient/util/setlog`.
2. Haga clic en **Establecer todo como inhabilitado** (este paso es opcional y garantiza que solo se recopilen los registros necesarios).
3. Vaya al registro de App Protection.
4. Para establecer el nivel de registro de App Protection en Detallado, haga clic con el botón secundario del ratón y seleccione Detallado (solo se registran las advertencias y los errores).
5. Amplíe la clase App Protection y haga clic con el botón secundario en su elemento secundario. Seleccione **Grupo > Heredado**.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

6. Habilite los registros para **wfica**. Haga clic con el botón secundario en **wfica** y seleccione **Detallado**. Si App Protection no está instalado o no lo puede detectar **wfica**, obtendrá una entrada de registro similar a **[NCS] < P3563 > citrix-wfica: App Protection no instalado**.
7. Al iniciar la sesión, los registros se graban en el archivo que se menciona en la *Ruta de salida del registro* que haya establecido.



Solución de problemas genéricos

March 11, 2024

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

Los recursos habilitados con las directivas de App Protection no se muestran en las aplicaciones nativas

Si los recursos habilitados con las directivas de App Protection no se muestran en las aplicaciones nativas, siga estos pasos:

1. Actualice la aplicación Citrix Workspace a una versión más reciente si es anterior a la siguiente:
   - Aplicación Citrix Workspace 2108 para Linux
   - Aplicación Citrix Workspace 2203.1 LTSR para Windows
   - Aplicación Citrix Workspace 2002 para Windows
   - Aplicación Citrix Workspace 2305.1 para la Tienda Windows
   - Aplicación Citrix Workspace 2001 para Mac
2. Asegúrese de no haber instalado la aplicación Citrix Workspace en un sistema operativo Windows multisesión, como Windows 2K16 o Windows 2K22.
3. Si se cumplen las condiciones anteriores pero los recursos siguen sin mostrarse, recopile los registros y contacte con el servicio de asistencia técnica de Citrix. Para obtener más información sobre la recopilación de registros, consulte Recopilación de registros.

Los recursos habilitados con las directivas de App Protection no se muestran en el explorador web mientras se usa el almacén local

Si los recursos habilitados con las directivas de App Protection no se muestran en el explorador web mientras se usa el almacén local, siga estos pasos:

1. Asegúrese de que su versión de Delivery Controller no es anterior a la versión 1912.

   > **Nota:**
   >
   > App Protection no está disponible si usa un Delivery Controller con versión anterior a la 1912.

2. Si usa las versiones de 1912 a 2203 de StoreFront, verifique que ha habilitado la personalización de StoreFront. Para obtener más información sobre cómo habilitar la personalización de StoreFront, consulte Habilitar la personalización de StoreFront.
3. Si usa la versión 2308 de StoreFront o una posterior, no necesita habilitar la personalización de StoreFront. Compruebe si ha habilitado correctamente App Protection para el inicio híbrido en StoreFront mediante Inicio híbrido a través de StoreFront, versión 2308 o una posterior.
4. Verifique si ha habilitado correctamente las funciones de App Protection para el grupo de entrega.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

5. Si se cumplen las condiciones anteriores pero siguen sin mostrarse los recursos, recopile los registros y contacte con el servicio de asistencia técnica de Citrix. Para obtener más información sobre la recopilación de registros, consulte Recopilar registros para la aplicación Citrix Workspace y Recopilar registros para StoreFront.

No se puede establecer un entorno seguro al iniciar los recursos habilitados para App Protection

En el caso de la aplicación Citrix Workspace para Windows, la casilla de verificación **Iniciar App Protection después de la instalación** debe estar habilitada durante la instalación para garantizar que se inicien los servicios de App Protection y se establezca el entorno seguro. Si no activó la casilla de verificación **Iniciar App Protection después de la instalación** durante la instalación, el servicio de App Protection se inicia automáticamente al iniciar un recurso habilitado con las directivas de App Protection. Según la carga del sistema, App Protection podría tardar en iniciarse. A veces es posible que comience o que se agote el tiempo de espera. Por lo tanto, durante la instalación se recomienda seleccionar la casilla de verificación **Iniciar App Protection después de la instalación**. Por lo general, al iniciar de nuevo el recurso habilitado con App Protection se debe establecer la conexión segura. No obstante, si aún no puede iniciar el recurso habilitado con App Protection, siga estos pasos:

1. Abra el símbolo del sistema como administrador, ejecute el siguiente comando y compruebe si el servicio de App Protection se está ejecutando:

```
sc query AppProtectionSvc
<!--NeedCopy-->
```

2. Si el servicio de App Protection no se está ejecutando, ejecute el siguiente comando para iniciar el servicio:

```
sc start AppProtectionSvc
<!--NeedCopy-->
```

3. Si sigue apareciendo el error, recopile los registros y contacte con el servicio de asistencia técnica de Citrix. Para obtener más información sobre la recopilación de registros, consulte Recopilación de registros.

No se puede habilitar o inhabilitar App Protection

Si no puede habilitar o inhabilitar App Protection para un grupo de entrega local o en la nube mediante Web Studio o PowerShell, siga estos pasos:

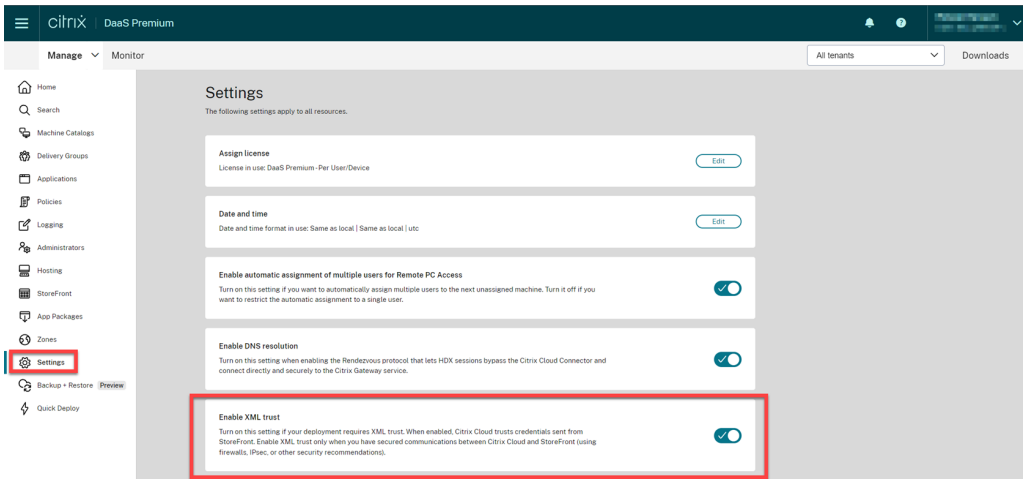
1. Compruebe si tiene la licencia requerida. Si las licencias requeridas no están disponibles, no puede habilitar App Protection.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

2. Si las licencias necesarias no están disponibles, obtenga las licencias necesarias y agréguelas.
3. Después de agregar las licencias, reinicie el servidor de licencias e intente habilitar App Protection de nuevo.
4. Si hay licencias válidas disponibles pero aún no puede habilitar o inhabilitar App Protection, ejecute el siguiente comando para comprobar si se habilitó `TrustRequestsSentToTheXmlServicePort`:

```
Get-BrokerSite | Select-Object
    TrustRequestsSentToTheXmlServicePort
<!--NeedCopy-->
```

5. Si `TrustRequestsSentToTheXmlServicePort` no está habilitado, habilite la confianza en XML mediante uno de los métodos siguientes:
   - **Mediante Web Studio:**
     a) Inicie sesión en su cuenta de Citrix DaaS y vaya a **Administrar** > **Parámetros** > **Habilitar la confianza en XML**.



     b) Active la opción **Habilitar confianza en XML**.
   - **Mediante PowerShell:** ejecute el siguiente comando para habilitar la confianza en XML:

```
Set-BrokerSite -TrustRequestsSentToTheXmlServicePort $true
<!--NeedCopy-->
```

6. Tras habilitar `TrustRequestsSentToTheXmlServicePort`, habilite App Protection de nuevo.
7. Si se cumplen las condiciones anteriores pero sigue sin poder habilitar o inhabilitar App Protection, contacte con el servicio de asistencia técnica de Citrix.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

Las directivas de App Protection no se aplican correctamente

1. Asegúrese de que se cumplen las siguientes condiciones:
    - Está usando una versión compatible de la aplicación Citrix Workspace.
    - El grupo de entrega tiene habilitadas las funciones correspondientes.
    - La función está instalada en el dispositivo de punto final.
    - La aplicación Citrix Workspace se ha instalado con el modificador / `includeappprotection` habilitado.
2. Si se cumplen las condiciones anteriores pero las directivas de App Protection siguen sin aplicarse correctamente, recopile los registros y contacte con el servicio de asistencia técnica de Citrix. Para obtener más información sobre la recopilación de registros, consulte Recopilar registros para la aplicación Citrix Workspace

Las capturas de pantalla no funcionan en ventanas que no son Citrix:

- Minimice o cierre las ventanas protegidas de Citrix, incluida la aplicación Citrix Workspace.

Solucionar problemas técnicos de detección de manipulación de directivas

March 11, 2024

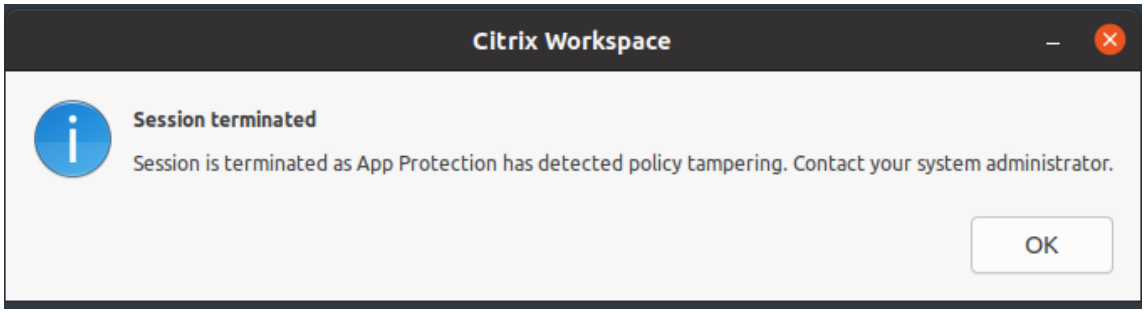
En la siguiente sección se describen algunos de los problemas a los que podría enfrentarse y cómo solucionarlos:

El archivo ICA está alterado y la sesión sigue ejecutándose

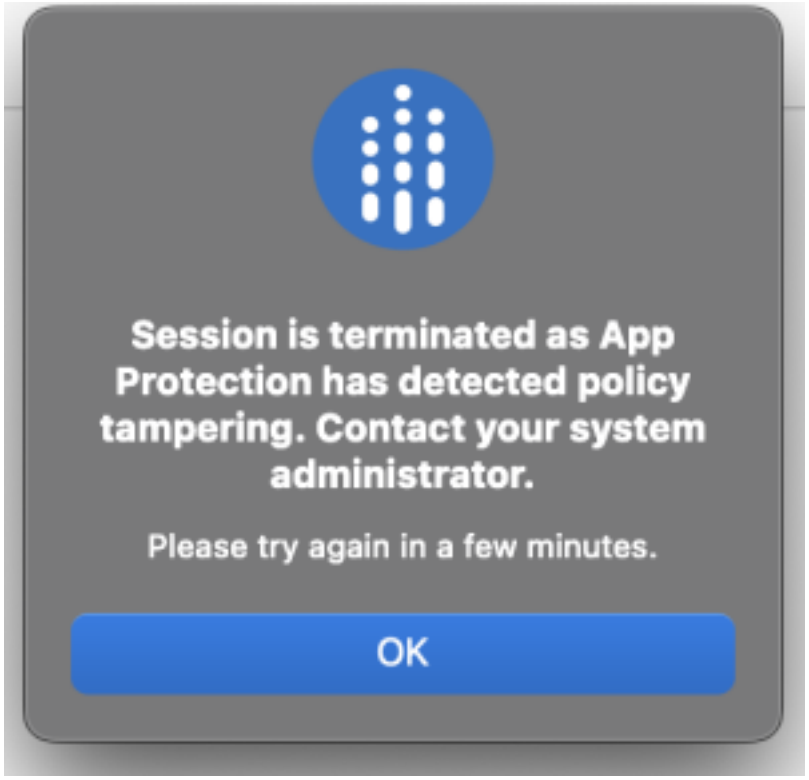
Si se manipula el archivo ICA de una sesión de escritorio o aplicación virtual que está habilitada con la función de detección de manipulación de directivas de App Protection, la sesión debe finalizar y mostrar uno de los siguientes mensajes de error:

- Aplicación Citrix Workspace para Linux

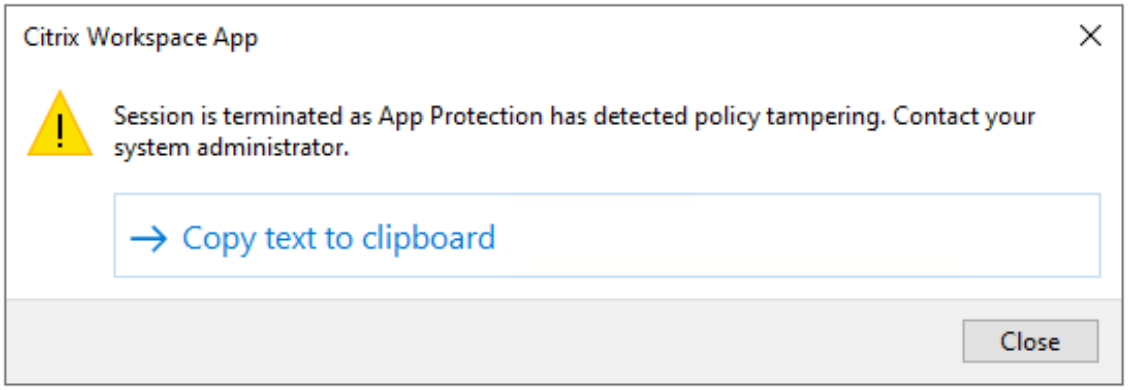
© 1999–2024 Cloud Software Group, Inc. All rights reserved.



- Aplicación Citrix Workspace para Mac



- Aplicación Citrix Workspace para Windows



Sin embargo, si la sesión se está ejecutando con el archivo ICA alterado y la detección de manipulación

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

de directivas está habilitada, lleve a cabo los siguientes pasos:

1. En Virtual Delivery Agent, haga lo siguiente:

   a) Ejecute el siguiente comando y compruebe si el servicio `ctxappprotectionsv` se está ejecutando:

   ```
   sc query ctxappprotectionsvc
   ```

   b) Si el servicio `ctxappprotectionsvc` no se está ejecutando, lleve a cabo los siguientes pasos para iniciarlo:

      i. Cambie el tipo de inicio del servicio `ctxappprotectionsvc` a automático mediante la ejecución del siguiente comando:

      ```
      sc config ctxappprotectionsvc start=auto
      ```

      ii. Inicie el servicio ejecutando el siguiente comando:

      ```
      sc start ctxappprotectionsvc
      ```

2. En el cliente, haga lo siguiente:

   a) Compruebe si el archivo *vdappp.dll* está en la ubicación de instalación de la aplicación Citrix Workspace. La ubicación de instalación predeterminada de la aplicación Citrix Workspace es la siguiente:

      - Windows: C:\Archivos de programa (x86)\Citrix\Cliente ICA
      - Linux: /opt/Citrix/ICAClient
      - Mac: no aplicable

   b) Para la aplicación Citrix Workspace para Windows, use *procexp.exe* y compruebe si el archivo *vdappp.dll* está cargado en *wfica32.exe*.

   c) Para la aplicación Citrix Workspace para Linux, compruebe si el archivo *vdappp.dll* está cargado en *wfica.exe*.

3. Si la sesión sigue ejecutándose, recopile los registros y contacte con la asistencia técnica de Citrix. Para obtener más información sobre la recopilación de registros, consulte Recopilación de registros.

La detección de manipulación de directivas deja de funcionar después de reiniciar Virtual Delivery Agent

Si reinicia el Virtual Delivery Agent y la función de detección de manipulación de directivas deja de funcionar, podría deberse a que el servicio App Protection no se está ejecutando después del reinicio. Realice los siguientes pasos en el Virtual Delivery Agent:

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

1. Ejecute el siguiente comando y compruebe si el servicio `ctxappprotectionsvc` se está ejecutando y está configurado en **automático**:

   ```
   sc query ctxappprotectionsvc
   ```

2. Si el servicio `ctxappprotectionsvc` no se está ejecutando, lleve a cabo los siguientes pasos para iniciarlo:

   a) Cambie el tipo de inicio del servicio `ctxappprotectionsvc` a **automático** mediante la ejecución del siguiente comando:

      ```
      sc config ctxappprotectionsvc start=auto
      ```

   b) Inicie el servicio ejecutando el siguiente comando:

      ```
      sc start ctxappprotectionsvc
      ```

3. Si la función de detección de manipulación de directivas sigue sin funcionar, recopile los registros y contacte con la asistencia técnica de Citrix. Para obtener más información sobre la recopilación de registros, consulte Recopilación de registros.

Solución de problemas técnicos de la verificación de la postura de App Protection

March 11, 2024

En la siguiente sección se describen algunos de los problemas a los que podría enfrentarse y cómo solucionarlos:

La sesión finalizó sin ningún mensaje de error

Si la sesión de escritorio o aplicación virtual finaliza bruscamente sin mostrar ningún mensaje de error, siga estos pasos:

1. Compruebe si la versión de la aplicación Citrix Workspace es anterior a una de las versiones siguientes:

   - Aplicación Citrix Workspace para Windows 2309
   - Aplicación Citrix Workspace para Mac 2308
   - Aplicación Citrix Workspace para Linux 2308

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

> **Nota:**
>
> Si la versión de la aplicación Citrix Workspace es anterior a las versiones enumeradas en el paso 1 y la función Comprobación de postura de App Protection está habilitada, la sesión de escritorio o aplicación virtual finaliza sin mostrar ningún mensaje de error. No obstante, si la versión de la aplicación Citrix Workspace es más reciente o igual a las versiones enumeradas en el paso 1 y la función Comprobación de la postura de App Protection está habilitada, la sesión de aplicaciones y escritorios virtuales finaliza mostrando un mensaje de error.

2. Compruebe si la función Comprobación de la postura de App Protection está habilitada.
3. Si la versión de la aplicación Citrix Workspace es más reciente o igual a las versiones anteriores y la función de Comprobación de la postura también está activa, recopile los registros y contacte con la asistencia técnica de Citrix. Para obtener más información sobre la recopilación de registros, consulte Recopilación de registros.

La Comprobación de la postura de App Protection está habilitada, pero la sesión no finaliza en las versiones anteriores

Por lo general, si la función de Comprobación de la postura de App Protection está habilitada y se conecta a través de una versión anterior de la aplicación Citrix Workspace, la sesión debe finalizar.

Pero si la sesión no finaliza, lleve a cabo los siguientes pasos:

1. En Virtual Delivery Agent, haga lo siguiente:
   a) Ejecute el siguiente comando y compruebe si el servicio `ctxappprotectionsvc` se está ejecutando:

      ```
      sc query ctxappprotectionsvc
      ```

   b) Si el servicio `ctxappprotectionsvc` no se está ejecutando, lleve a cabo los siguientes pasos para iniciarlo:
      i. Cambie el tipo de inicio de `ctxappprotectionsvc service` a **automático** ejecutando el siguiente comando:

         ```
         sc config ctxappprotectionsvc start=auto
         ```

      ii. Inicie el servicio ejecutando el siguiente comando:

         ```
         sc start ctxappprotectionsvc
         ```

2. Compruebe si los valores de Comprobación de la postura que introdujo tienen uno de los siguientes prefijos:

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

- Para la aplicación Citrix Workspace para Windows, `windows-`
- Aplicación Citrix Workspace para Linux, `linux-`
- Aplicación Citrix Workspace para Mac, `mac-`

3. Compruebe si los valores de Comprobación de la postura se agregan correctamente según la plataforma correspondiente, ya que son específicos de cada plataforma.
4. Compruebe la ubicación de `reg` (`Computer\HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Citrix\AppProtectionPolicies`) para verificar si la Comprobación de la postura está sincronizada con el Virtual Delivery Agent.
5. Si se cumplen todas las condiciones anteriores y la sesión sigue conectada para las versiones anteriores de la aplicación Citrix Workspace, recopile los registros y contacte con la asistencia técnica de Citrix. Para obtener más información sobre la recopilación de registros, consulte Recopilación de registros.

La Comprobación de la postura de App Protection funciona en una plataforma pero no en otra

A veces, la función de Comprobación de la postura de App Protection puede funcionar en una plataforma y no en otra. Por ejemplo, la función Comprobación de la postura de App Protection funciona en la aplicación Citrix Workspace para Windows, pero no en la aplicación Citrix Workspace para Linux.

En situaciones como estas, lleve a cabo los siguientes pasos:

1. Compruebe si los valores de Comprobación de la postura que introdujo tienen uno de los siguientes prefijos:
   - Para la aplicación Citrix Workspace para Windows, `windows-`
   - Aplicación Citrix Workspace para Linux, `linux-`
   - Aplicación Citrix Workspace para Mac, `mac-`
2. Compruebe si los valores de Comprobación de la postura se agregan correctamente según la plataforma correspondiente, ya que son específicos de cada plataforma.
3. Compruebe la ubicación de `reg` (`Computer\HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Citrix\AppProtectionPolicies`) en el Virtual Delivery Agent para verificar si la Comprobación de la postura está sincronizada con el Virtual Delivery Agent. Deben coincidir con lo que se configuró en Studio.
4. Si se cumplen todas las condiciones anteriores y la sesión sigue conectada para las versiones anteriores de la aplicación Citrix Workspace, recopile los registros y contacte con la asistencia técnica de Citrix. Para obtener más información sobre la recopilación de registros, consulte Recopilación de registros.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

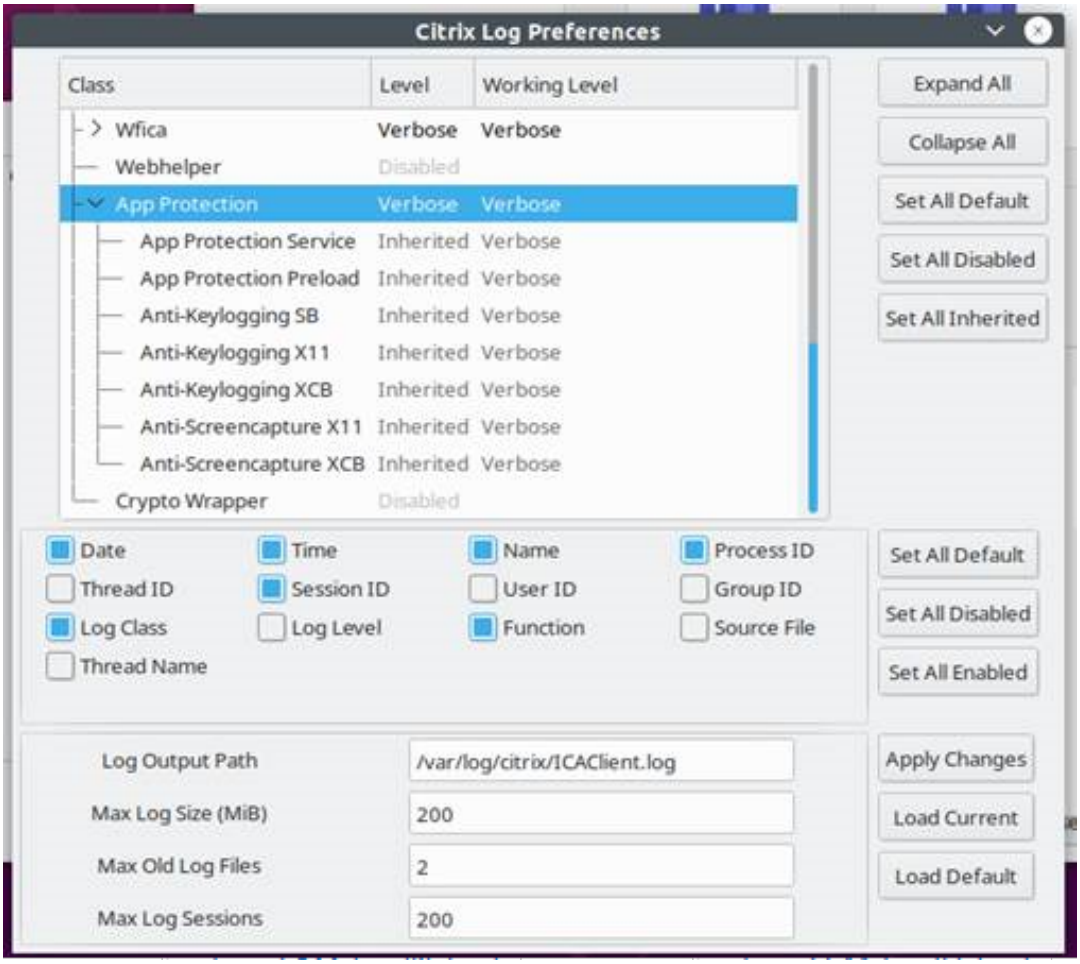
Recopilación de registros

March 11, 2024

- Para recopilar registros para la aplicación Citrix Workspace para Windows, consulte Recopilación de registros para Windows.
- Para recopilar registros para la aplicación Citrix Workspace para Mac, consulte Recopilación de registros para Mac.
- Para recopilar registros para la aplicación Citrix Workspace para Linux, lleve a cabo los siguientes pasos:

  1. Ejecute el registro establecido ejecutable que se encuentra en el directorio *util* de la instalación. Por ejemplo, */opt/Citrix/ICAClient/util/setlog*.
  2. (Opcional) Haga clic en **Establecer todo inhabilitado** y asegúrese de que solo se recopilen los registros necesarios.
  3. Vaya al registro de App Protection.
  4. Para establecer el nivel de registro de App Protection en Detallado, haga clic con el botón secundario y seleccione **Detallado** (solo se registran las advertencias y los errores).
  5. Amplíe la clase App Protection y haga clic con el botón secundario en su elemento secundario. Seleccione **Grupo** > **Heredado**.
  6. Use la captura de registros de Linux (desde *install dir*, inicie *util/setlog*) y cambie el nivel de registro del canal virtual a Detallado.
  7. Habilite los registros para **wfica**. Haga clic con el botón secundario en **wfica** y seleccione **Detallado**. Si App Protection no está instalado o no lo puede detectar **wfica**, obtendrá una entrada de registro similar a **[NCS] < P3563 > citrix-wfica: App Protection no instalado**.
  8. Haga clic en **wfica** y cambie el nivel de registro del **controlador Winstation** a **Detallado**.
  9. Al iniciar la sesión, los registros se graban en el archivo que se menciona en la Ruta de salida del registro establecido.

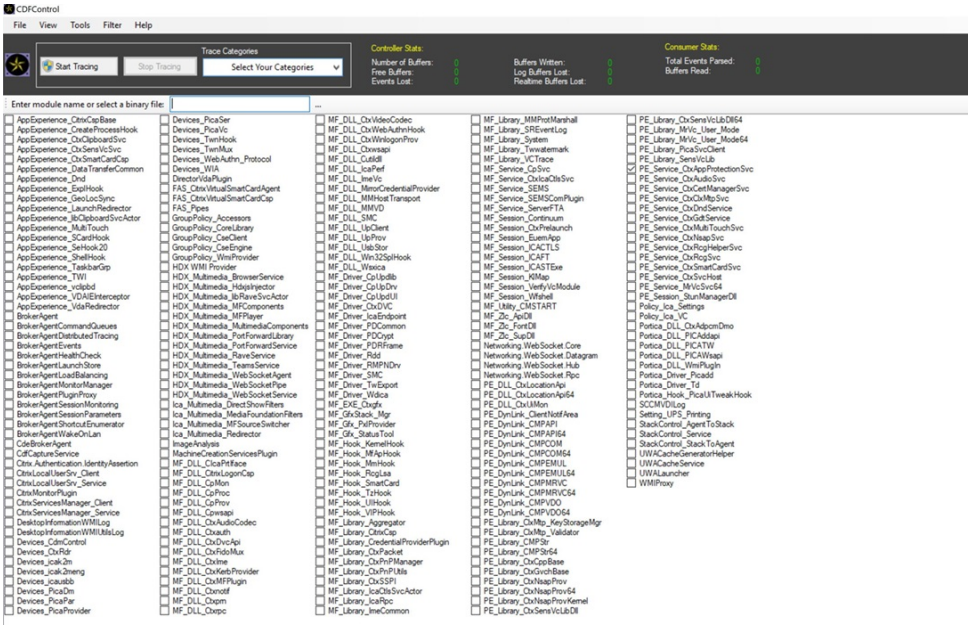
© 1999–2024 Cloud Software Group, Inc. All rights reserved.



- Para recopilar registros para el Virtual Delivery Agent, lleve a cabo los siguientes pasos:

  1. Para realizar el rastreo del servicio App Protection a través del control CDF, seleccione todos los módulos.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.



2. En determinados casos, es posible que tengamos que capturar el rastreo de CDF desde una máquina diferente. Para realizar el rastreo de CDF, consulte CTX237216.

Contextual App Protection para Workspace

March 11, 2024

Contextual App Protection ofrece la posibilidad de aplicar directivas de App Protection de forma condicional a un subconjunto de usuarios, en función de sus características, sus dispositivos y la estrategia de red.

Implementar Contextual App Protection

Puede implementar Contextual App Protection por medio de los filtros de conexión definidos en la regla de directiva de acceso con intermediario. Las directivas de acceso con intermediario definen las reglas que controlan el acceso de un usuario a grupos de escritorios. La directiva comprende un conjunto de reglas. Cada regla se refiere a un único grupo de entrega y tiene un conjunto de filtros de conexión y controles de derechos de acceso.

Los usuarios pueden acceder a un grupo de entrega cuando los detalles de su conexión coinciden con los filtros de conexión de una o más reglas de la directiva de acceso con intermediario. De forma predeterminada, los usuarios no tienen acceso a ningún grupo de entrega de un sitio. Puede crear más directivas de acceso con intermediario en función de sus requisitos. Se pueden aplicar varias reglas a un mismo grupo de entrega. Para obtener más información, consulte New-BrokerAccessPolicyRule.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

Los siguientes parámetros de la regla de directiva de acceso con intermediario ofrecen la flexibilidad necesaria para habilitar App Protection en contexto si la conexión del usuario coincide con los filtros de conexión definidos en la regla de directiva de acceso:

- `AppProtectionKeyLoggingRequired`
- `AppProtectionScreenCaptureRequired`

Utilice las directivas de Smart Access a las que se hace referencia en las reglas de la directiva de acceso con intermediario para refinar los filtros de conexión. Para comprender cómo usar las directivas de Smart Access para configurar Contextual App Protection, consulte los casos que se explican en este artículo.

Casos de Contextual App Protection

Estos son algunos de los casos sobre cómo puede habilitar Contextual App Protection:

- Habilitar App Protection para usuarios externos que llegan a través de Access Gateway
- Habilitar App Protection para dispositivos que no son de confianza
- Habilitar App Protection en función de los resultados de Device Posture
- Habilitar App Protection para grupos de usuarios específicos

Requisitos previos

March 11, 2024

Asegúrese de tener lo siguiente:

- Servicio de ubicación de red (NLS) para casos basados en la ubicación de red del usuario
- Requisitos del sistema de licencias:
  - App Protection para DaaS
  - Derecho de uso de la autenticación adaptable para casos con directivas de Smart Access.

Caso 1

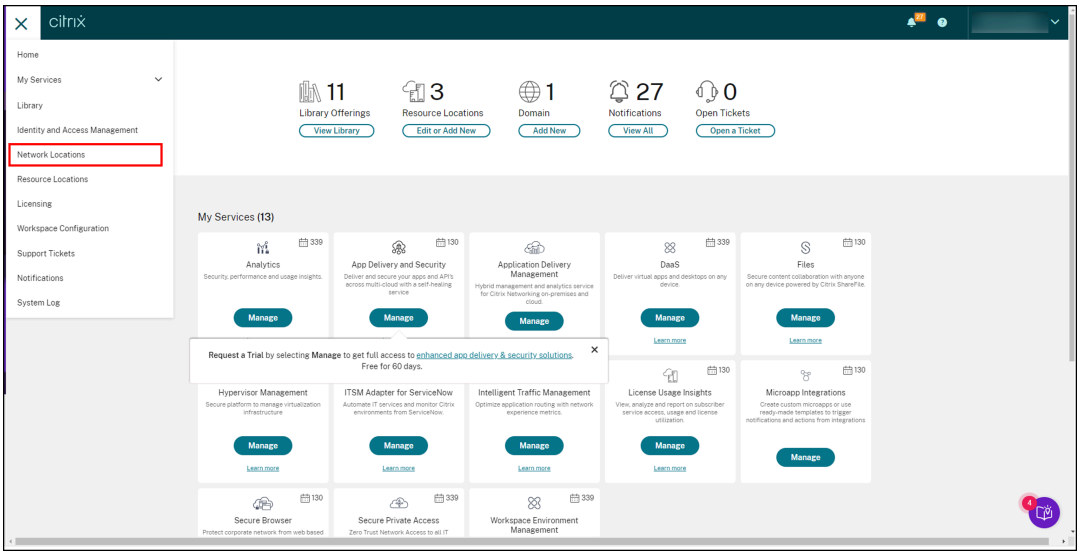
April 10, 2024

Este caso cubre cómo habilitar App Protection para usuarios externos que llegan a través de Access Gateway.

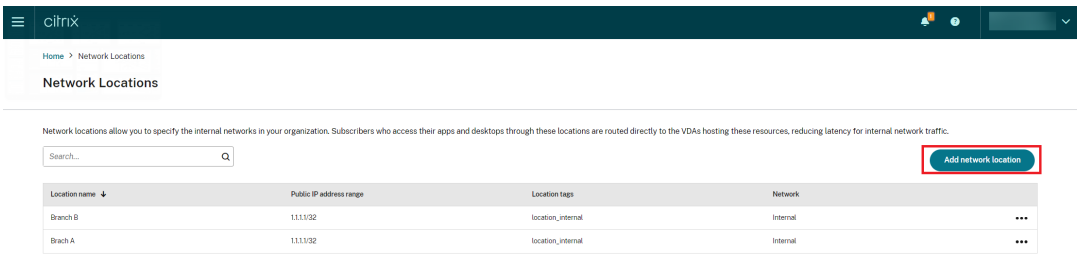
© 1999–2024 Cloud Software Group, Inc. All rights reserved.

1. Configure la autenticación adaptable.
2. Configure el acceso adaptable en función de la ubicación de su red.

   a) Inicie sesión en Citrix Cloud y vaya a **Ubicaciones de red**.



   b) Haga clic en **Agregar ubicación de red**.



   Aparece la pantalla**Agregar una ubicación de red**.

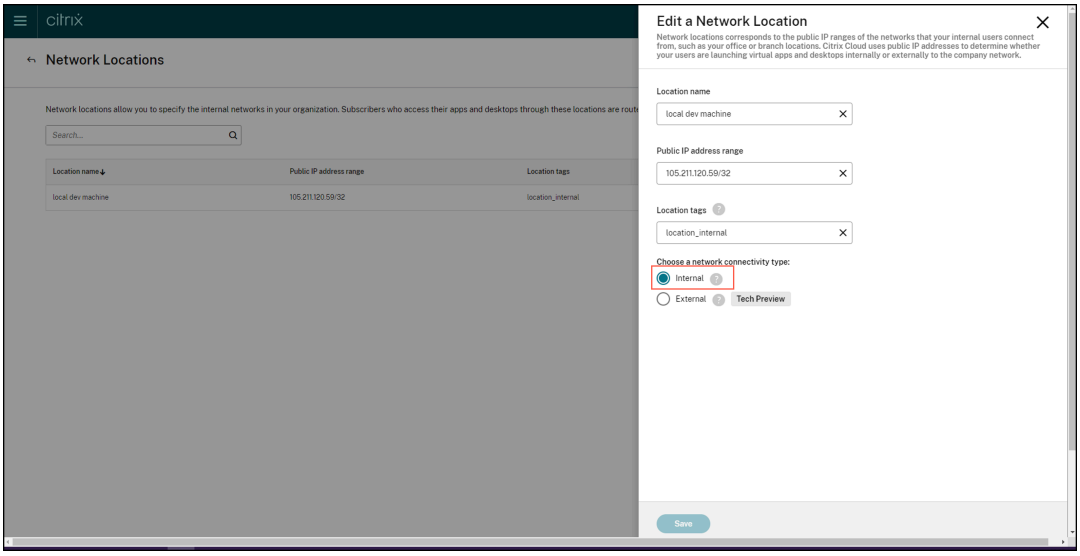
   c) En el campo **Nombre de la ubicación**, introduzca el nombre de la ubicación correspondiente.

   d) En el campo **Intervalo de direcciones IP públicas**, introduzca la dirección IP o subred de la red que quiera considerar como red interna.

   e) En el campo **Etiquetas de ubicación**, introduzca **location_internal**. Para obtener más información sobre la etiqueta de ubicación, consulte Etiquetas de ubicación.

   f) En **Elija un tipo de conectividad de red**, seleccione *Interna*.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.



Si inicia sesión en el almacén de la nube desde un dispositivo cuya dirección IP está configurada como *interna* en la opción **Elija un tipo de conectividad de red**, la conexión se considera una conexión interna.

3. Configurar las reglas de la directiva de acceso con intermediario

   Para cada grupo de entrega, se crean dos directivas de acceso con intermediario de forma predeterminada. Una directiva es para las conexiones que llegan a través de Access Gateway, y la otra es para conexiones directas. Puede habilitar App Protection solo para las conexiones que llegan a través de Access Gateway, que son las conexiones externas. Siga estos pasos para configurar las reglas de la directiva de acceso con intermediario:

   a) Instale el SDK de PowerShell para Citrix y conéctese a la API de la nube como se explica en el blog de Citrix Getting started with PowerShell automation for Citrix Cloud.

   b) Ejecute el comando `Get-BrokerAccessPolicyRule`.

      Se muestra una lista de todas las directivas de acceso con intermediario para todos los grupos de entrega presentes.

   c) Busque el **DesktopGroupUid** del grupo de entrega que quiere cambiar.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

```
PS C:\Windows\System32> Get-BrokerAccessPolicyRule


AllowRestart                      : True
AllowedConnections                : ViaAG
AllowedProtocols                  : {HDX, RDP}
AllowedUsers                      : AnyAuthenticated
AppProtectionKeyLoggingRequired   : False
AppProtectionScreenCaptureRequired : False
Description                       :
DesktopGroupName                  : App Protection
DesktopGroupUid                   : 15
Enabled                           : True
ExcludedClientIPFilterEnabled     : False
ExcludedClientIPs                 : {}
ExcludedClientNameFilterEnabled   : False
ExcludedClientNames               : {}
ExcludedSmartAccessFilterEnabled  : False
ExcludedSmartAccessTags           : {}
ExcludedUserFilterEnabled         : False
ExcludedUsers                     : {}
HdxSslEnabled                     : False
IncludedClientIPFilterEnabled     : False
IncludedClientIPs                 : {}
IncludedClientNameFilterEnabled   : False
IncludedClientNames               : {}
IncludedSmartAccessFilterEnabled  : True
IncludedSmartAccessTags           : {}
IncludedUserFilterEnabled         : True
IncludedUsers                     : {}
MetadataMap                       : {[IfBuiltInAccessPolicyRuleOfDeliveryGroup, True], [IfCreatedByOrchAccessPolicyRuleOfDeliveryGroup, True]}
Name                              : App Protection_AG
Uid                               : 37

AllowRestart                      : True
AllowedConnections                : NotViaAG
AllowedProtocols                  : {HDX, RDP}
AllowedUsers                      : AnyAuthenticated
AppProtectionKeyLoggingRequired   : False
AppProtectionScreenCaptureRequired : False
Description                       :
DesktopGroupName                  : App Protection
DesktopGroupUid                   : 15
Enabled                           : True
ExcludedClientIPFilterEnabled     : False
ExcludedClientIPs                 : {}
ExcludedClientNameFilterEnabled   : False
ExcludedClientNames               : {}
ExcludedSmartAccessFilterEnabled  : False
ExcludedSmartAccessTags           : {}
ExcludedUserFilterEnabled         : False
ExcludedUsers                     : {}
HdxSslEnabled                     : False
IncludedClientIPFilterEnabled     : False
IncludedClientIPs                 : {}
IncludedClientNameFilterEnabled   : False
IncludedClientNames               : {}
IncludedSmartAccessFilterEnabled  : True
IncludedSmartAccessTags           : {}
IncludedUserFilterEnabled         : True
IncludedUsers                     : {}
MetadataMap                       : {[IfBuiltInAccessPolicyRuleOfDeliveryGroup, True], [IfCreatedByOrchAccessPolicyRuleOfDeliveryGroup, True]}
Name                              : App Protection_Direct
Uid                               : 36
```

d) Ejecute este comando con **DesktopGroupUid** para obtener directivas aplicables al grupo de entrega. Hay al menos dos directivas, una en la que *AllowedConnections* tiene *ViaAG* y otra, *NotViaAG*.

```
Get-BrokerAccessPolicyRule -DesktopGroupUid 15
```

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

```
PS C:\Windows\System32> Get-BrokerAccessPolicyRule -DesktopGroupUid 15


AllowRestart                      : True
AllowedConnections                : ViaAG
AllowedProtocols                  : {HDX, RDP}
AllowedUsers                      : AnyAuthenticated
AppProtectionKeyLoggingRequired   : False
AppProtectionScreenCaptureRequired : False
Description                       :
DesktopGroupName                  : App Protection
DesktopGroupUid                   : 15
Enabled                           : True
ExcludedClientIPFilterEnabled     : False
ExcludedClientIPs                 : {}
ExcludedClientNameFilterEnabled   : False
ExcludedClientNames               : {}
ExcludedSmartAccessFilterEnabled  : False
ExcludedSmartAccessTags           : {}
ExcludedUserFilterEnabled         : False
ExcludedUsers                     : {}
HdxSslEnabled                     : False
IncludedClientIPFilterEnabled     : False
IncludedClientIPs                 : {}
IncludedClientNameFilterEnabled   : False
IncludedClientNames               : {}
IncludedSmartAccessFilterEnabled  : True
IncludedSmartAccessTags           : {}
IncludedUserFilterEnabled         : True
IncludedUsers                     : {}
MetadataMap                       : {[IfBuiltInAccessPolicyRuleOfDeliveryGroup, True], [IfCreatedByOrchAccessPolicyRuleOfDeliveryGroup, True]}
Name                              : App Protection_AG
Uid                               : 37

AllowRestart                      : True
AllowedConnections                : NotViaAG
AllowedProtocols                  : {HDX, RDP}
AllowedUsers                      : AnyAuthenticated
AppProtectionKeyLoggingRequired   : False
AppProtectionScreenCaptureRequired : False
Description                       :
DesktopGroupName                  : App Protection
DesktopGroupUid                   : 15
Enabled                           : True
ExcludedClientIPFilterEnabled     : False
ExcludedClientIPs                 : {}
ExcludedClientNameFilterEnabled   : False
ExcludedClientNames               : {}
ExcludedSmartAccessFilterEnabled  : False
ExcludedSmartAccessTags           : {}
ExcludedUserFilterEnabled         : False
ExcludedUsers                     : {}
HdxSslEnabled                     : False
IncludedClientIPFilterEnabled     : False
IncludedClientIPs                 : {}
IncludedClientNameFilterEnabled   : False
IncludedClientNames               : {}
IncludedSmartAccessFilterEnabled  : True
IncludedSmartAccessTags           : {}
IncludedUserFilterEnabled         : True
IncludedUsers                     : {}
MetadataMap                       : {[IfBuiltInAccessPolicyRuleOfDeliveryGroup, True], [IfCreatedByOrchAccessPolicyRuleOfDeliveryGroup, True]}
Name                              : App Protection_Direct
Uid                               : 36
```

En la captura de pantalla, verá dos directivas:

- App Protection_AG: *AllowedConnections* con *ViaAG*, que es la directiva de conexiones a través de Access Gateway
- App Protection_Direct: *AllowedConnections* con *NotViaAG*, que es la directiva para conexiones que no son a través de Access Gateway

4. Habilite las directivas de App Protection solo para las conexiones externas e inhabilítelas para las conexiones internas mediante estos comandos:

   - `Set-BrokerAccessPolicyRule "App Protection_AG"-IncludedSmartAccessFilt $true -IncludedSmartAccessTags Workspace:LOCATION_internal -AppProtectionScreenCaptureRequired $false -AppProtectionKeyLoggingRequ $false`
   - `New-BrokerAccessPolicyRule "App Protection_AG_Exclude"-ExcludedsmartAc $true -ExcludedSmartAccessTags Workspace:LOCATION_internal -AppProtectionScreenCaptureRequired $true -AppProtectionKeyLoggingRequi $true -DesktopGroupUid 15 -AllowedConnections ViaAG -AllowedProtocols HDX, RDP`
   - `Remove-BrokerAccessPolicyRule "App Protection_Direct”`

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

5. Verificación:

   Cierre sesión en la aplicación Citrix Workspace e iníciela de nuevo. Inicie el recurso protegido desde una conexión externa. Verá que se aplican las directivas de App Protection. Inicie el mismo recurso desde una conexión interna, un dispositivo dentro del intervalo de direcciones IP configurado en el primer paso. Verá que las directivas de App Protection están inhabilitadas.

Caso 2

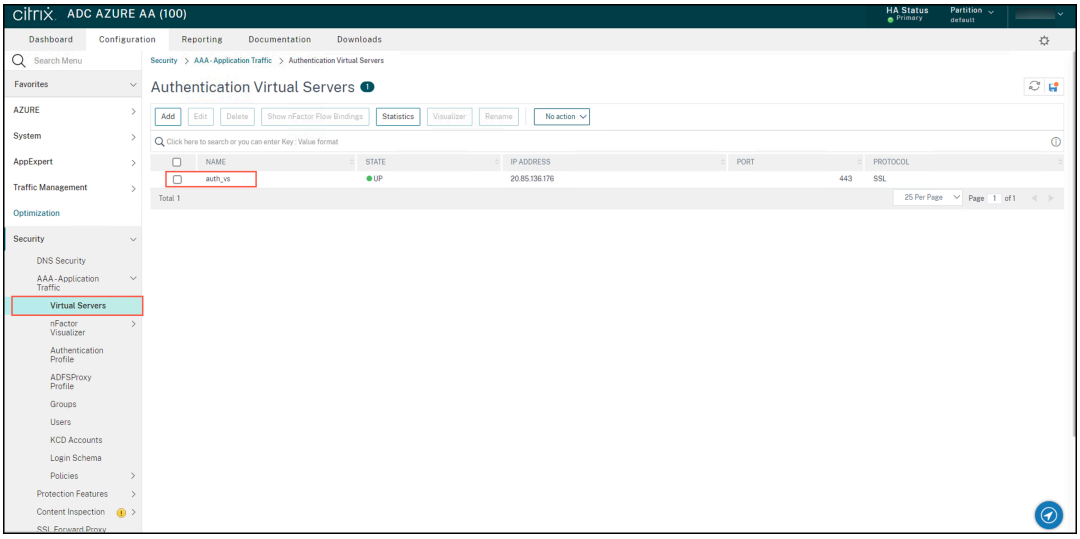
April 10, 2024

Este caso trata de cómo habilitar App Protection para dispositivos que no son de confianza.

Hay muchas definiciones de dispositivos de confianza y de dispositivos que no son de confianza. Para este caso, consideremos un dispositivo de confianza si el análisis de Endpoint Analysis (EPA) se realiza correctamente. Todos los demás dispositivos se consideran dispositivos que no son de confianza.

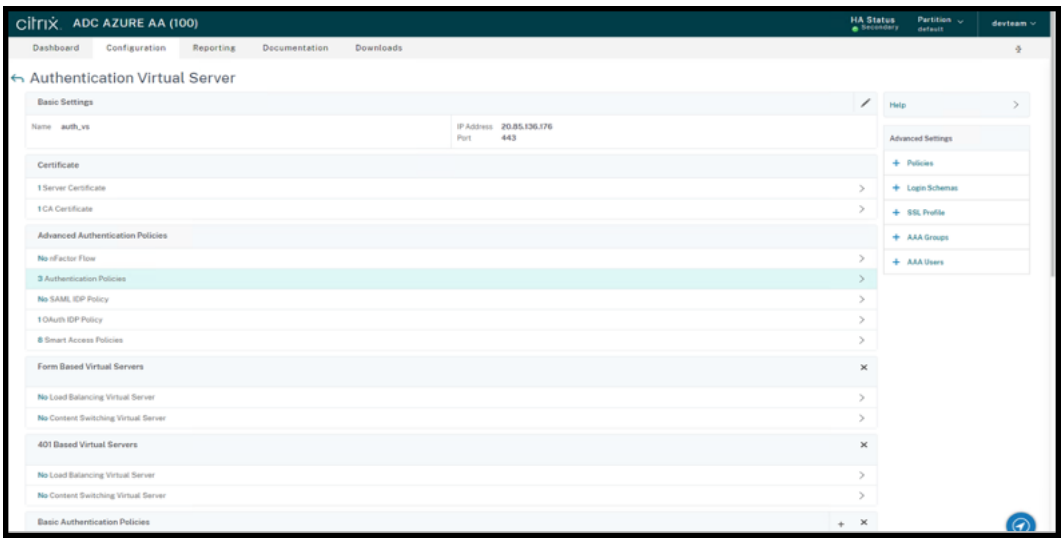
1. Configure la autenticación adaptable.
2. Cree una directiva de autenticación con el análisis de EPA mediante estos pasos:

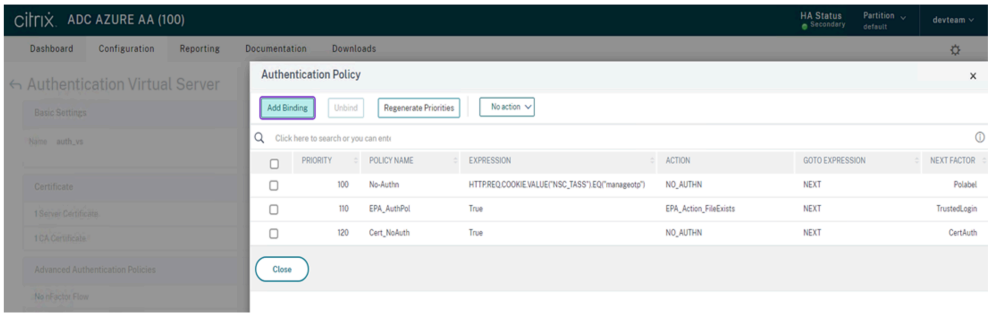
   a) Inicie sesión en la interfaz de usuario de administración de Citrix ADC. En la ficha **Configuration**, vaya a **Security > AAA-Application Traffic > Virtual Servers**. Haga clic en el servidor virtual que quiera usar; *auth_vs* en este caso.



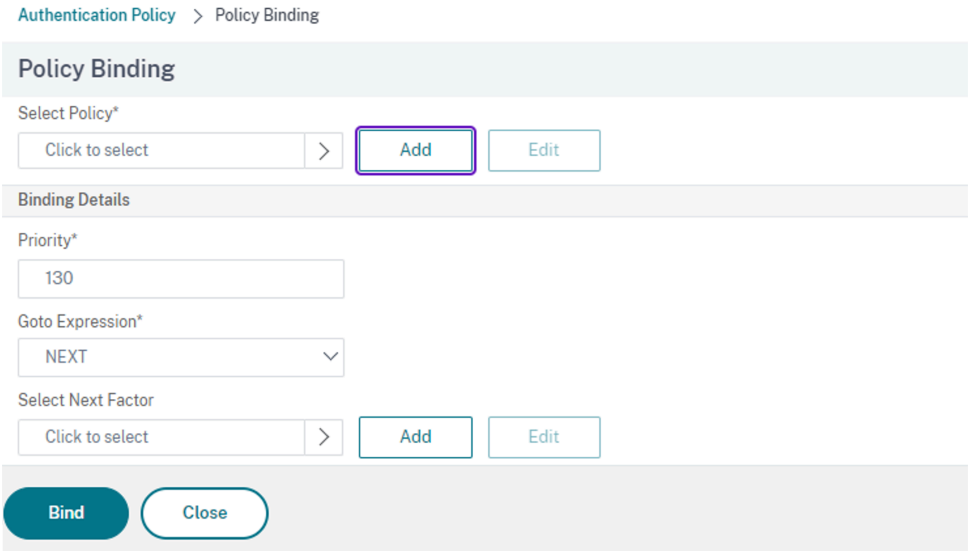
   b) Vaya a **Authentication Policies > Add Binding**.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.



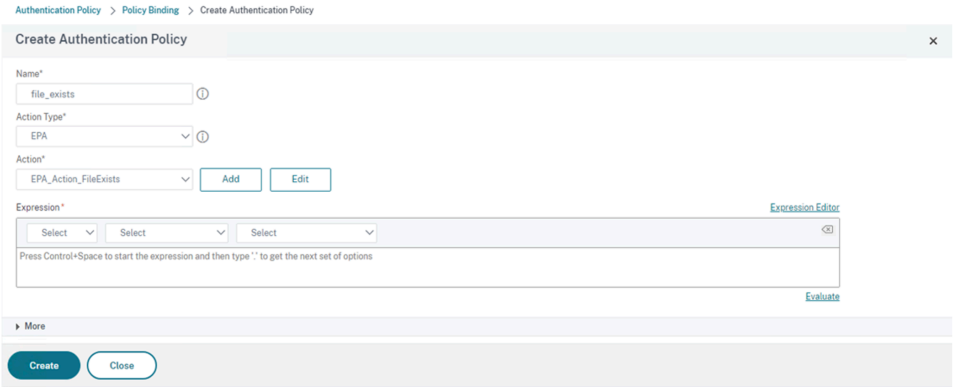


c) Haga clic en **Add** para crear una directiva.

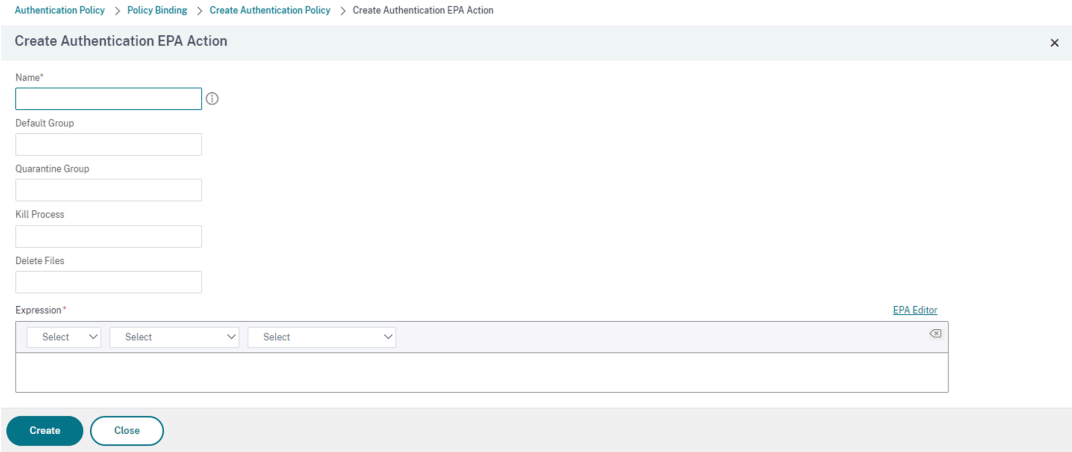


d) Cree una directiva de autenticación basada en el análisis de EPA. Introduzca el nombre de la directiva. En **Action Type**, seleccione *EPA*. Haga clic en **Add** para crear una acción.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.



Aparecerá la pantalla **Create Authentication EPA Action**.



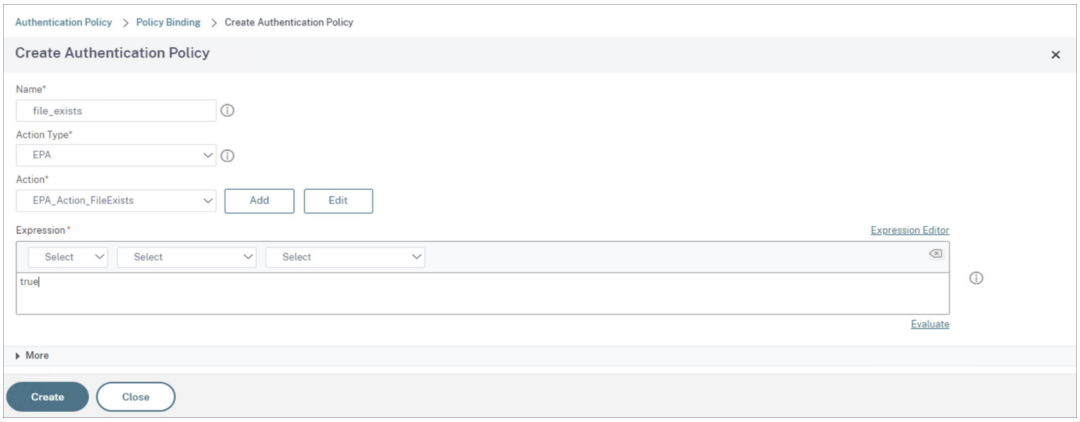
e) En la pantalla **Create Authentication EPA Action**, introduzca estos detalles y haga clic en **Create** para crear una acción:

- **Name**: El nombre de la acción de EPA. En este caso, *EPA_Action_FileExists*.
- **Default Group**: Introduzca el nombre del grupo predeterminado. Si la expresión EPA es *True*, los usuarios se agregan al grupo predeterminado. Aquí, **Default Group** es *FileExists*.
- **Quarantine Group**: Introduzca el nombre del grupo de cuarentena. Si la expresión de EPA es *False*, los usuarios se agregan al grupo de cuarentena.
- **Expression**: Agregue la expresión de EPA que quiera analizar. En este ejemplo, consideramos que el análisis de EPA es correcto si hay un archivo en particular: `sys.client_expr("file_0_C:\\\\\epa\\\\\avinstalled.txt")`

Regresará a la pantalla **Create Authentication Policy**.

f) Escriba **true** en el editor de expresiones y haga clic en **Create**.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.



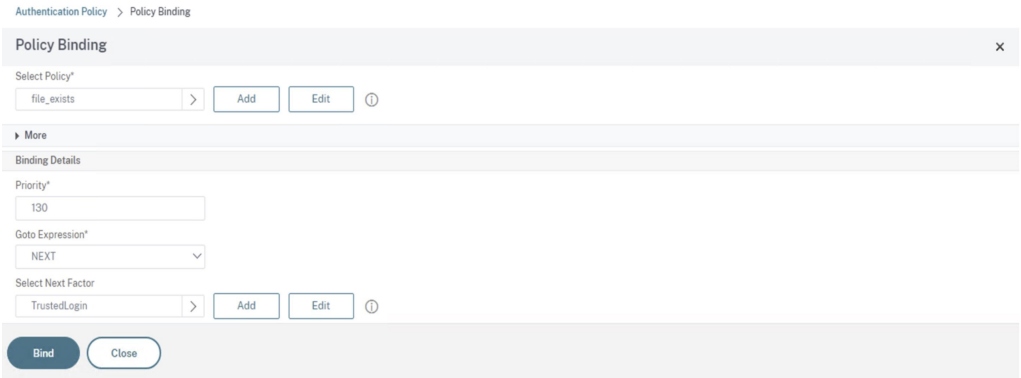
Regresará a la pantalla **Policy Binding**.

g) En la pantalla **Policy Binding**, haga lo siguiente:

   i. En **Goto Expression**, seleccione **NEXT**.

   ii. En la sección **Select Next Factor**, seleccione la directiva de LDAP que configuró para la autenticación en el Application Delivery Controller (ADC).

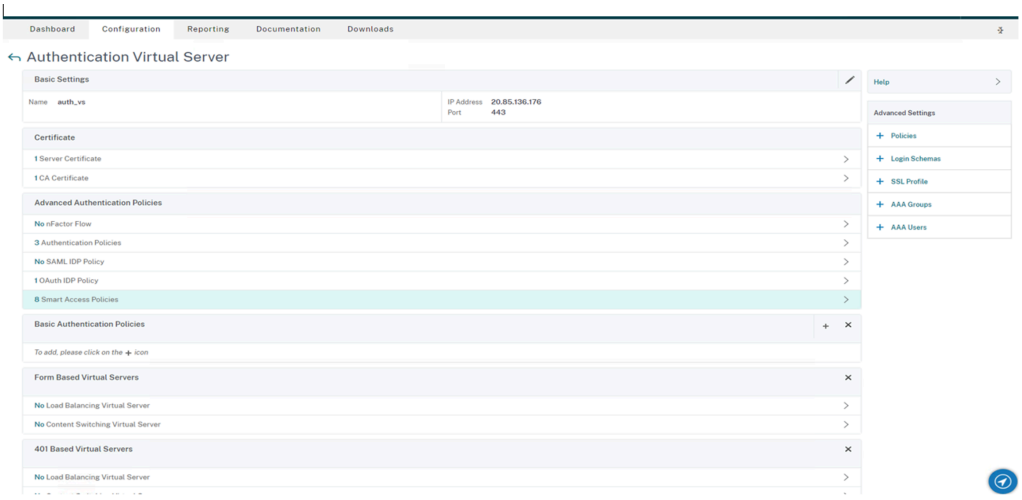
   iii. Haga clic en **Bind**.



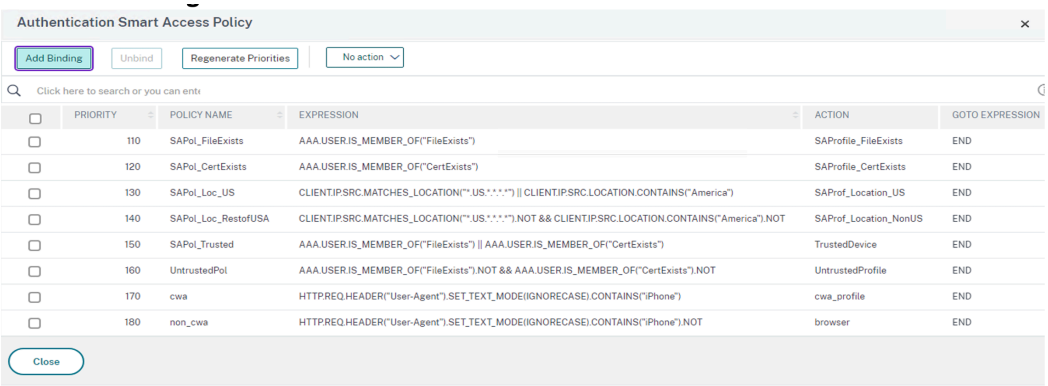
3. Cree una directiva de Smart Access para dispositivos de confianza:

   a) Seleccione **Smart Access Policies** en la página **Authentication Virtual Server** del servidor *auth_vs*.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.



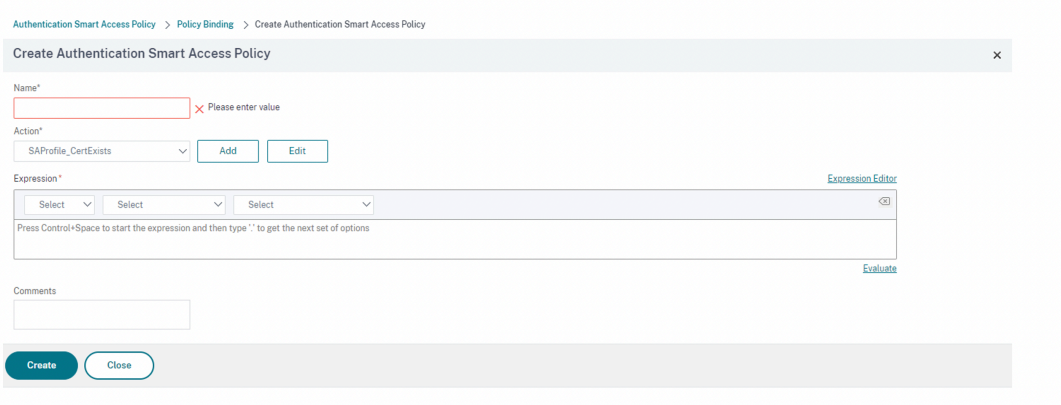
b) Haga clic en **Add Binding**.



c) En la pantalla **Policy Binding**, haga clic en **Add** en la sección **Select Policy**.

Aparece la pantalla **Create Authentication Smart Access Policy**.

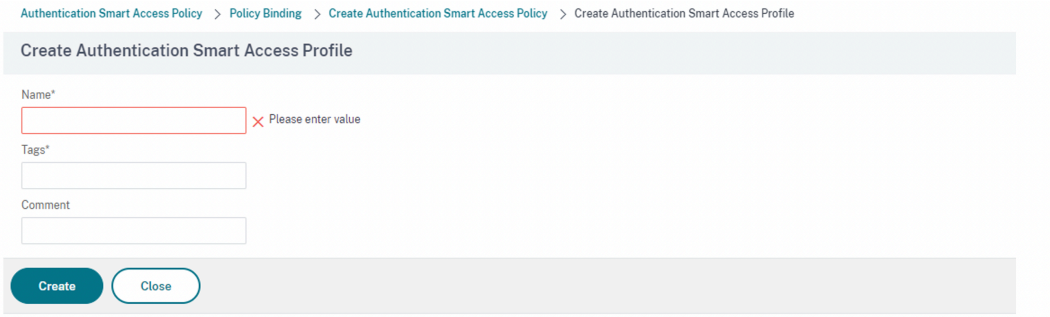
© 1999–2024 Cloud Software Group, Inc. All rights reserved.



d) En la pantalla **Create Authentication Smart Access Policy**, introduzca el nombre de la directiva de Smart Access en **Name** y haga clic en **Add** para crear un perfil de Smart Access.

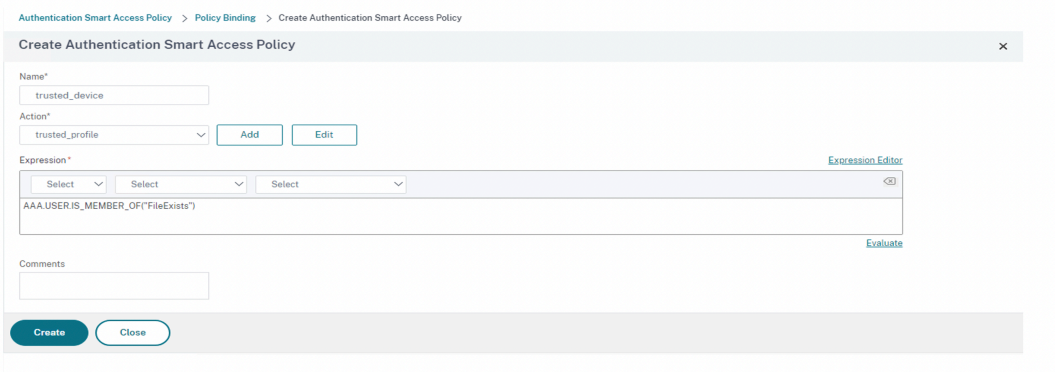
Aparecerá la pantalla **Create Authentication Smart Access Profile**.

e) Agregue el nombre de la acción en **Name**. Introduzca *trusted* en **Tags**. Luego se hace referencia a la etiqueta en la regla de la directiva de acceso con intermediario para su configuración. Haga clic en **Crear**.



Regresará a la pantalla **Create Authentication Smart Access Policy**.

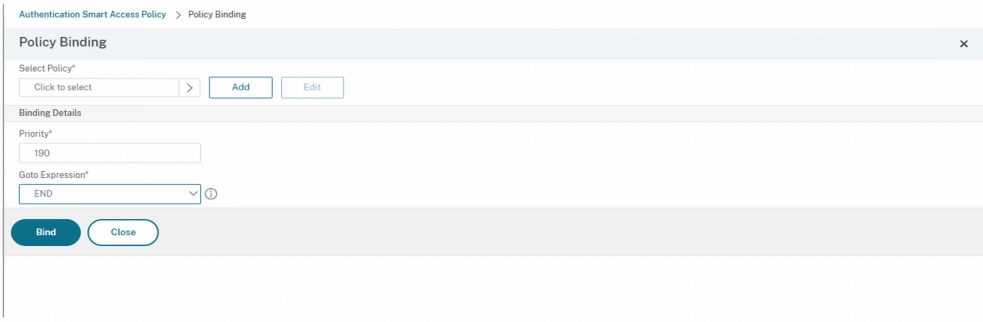
f) En la sección **Expression**, introduzca la expresión para la que quiere insertar la etiqueta. En este caso, como la etiqueta se inserta para dispositivos de confianza, introduzca `AAA.USER.IS_MEMBER_OF("FileExists")`. Haga clic en **Crear**.



© 1999–2024 Cloud Software Group, Inc. All rights reserved.

Regresará a la pantalla **Policy Binding**.

g) En **Goto Expression**, seleccione *End* y haga clic en **Bind**.



4. Cree una directiva de Smart Access para dispositivos que no sean de confianza:

   a) Siga las instrucciones del paso anterior, excepto los subpasos **v** y **vi**.

   b) Para el subpaso **v**, en la pantalla **Create Authentication Smart Access Profile**, agregue un nombre para la acción en **Name**. Introduzca *untrusted* en **Tags**. Luego se hace referencia a la etiqueta en la regla de la directiva de acceso con intermediario para su configuración. Haga clic en **Crear**.

   c) Para el subpaso **vi**, en la sección **Expression** de la pantalla **Create Authentication Smart Access Policy**, introduzca la expresión para la que quiere insertar la etiqueta. En este caso, como la etiqueta se inserta para dispositivos que no son de confianza, introduzca `AAA.USER.IS_MEMBER_OF("FileExists").NOT`.

5. Configure las reglas de directivas de acceso con intermediario:

   a) Instale el SDK de PowerShell para Citrix y conéctese a la API de la nube como se explica en el blog de Citrix Getting started with PowerShell automation for Citrix Cloud.

   b) Ejecute el comando `Get-BrokerAccessPolicyRule`.

      Se muestra una lista de todas las directivas de acceso con intermediario para todos los grupos de entrega presentes.

   c) Busque el **DesktopGroupUid** del grupo de entrega que quiere cambiar.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

```
PS C:\Windows\System32> Get-BrokerAccessPolicyRule


AllowRestart                      : True
AllowedConnections                : ViaAG
AllowedProtocols                  : {HDX, RDP}
AllowedUsers                      : AnyAuthenticated
AppProtectionKeyLoggingRequired   : False
AppProtectionScreenCaptureRequired : False
Description                       :
DesktopGroupName                  : App Protection
DesktopGroupUid                   : 15
Enabled                           : True
ExcludedClientIPFilterEnabled     : False
ExcludedClientIPs                 : {}
ExcludedClientNameFilterEnabled   : False
ExcludedClientNames               : {}
ExcludedSmartAccessFilterEnabled  : False
ExcludedSmartAccessTags           : {}
ExcludedUserFilterEnabled         : False
ExcludedUsers                     : {}
HdxSslEnabled                     : False
IncludedClientIPFilterEnabled     : False
IncludedClientIPs                 : {}
IncludedClientNameFilterEnabled   : False
IncludedClientNames               : {}
IncludedSmartAccessFilterEnabled  : True
IncludedSmartAccessTags           : {}
IncludedUserFilterEnabled         : True
IncludedUsers                     : {}
MetadataMap                       : {[IfBuiltInAccessPolicyRuleOfDeliveryGroup, True], [IfCreatedByOrchAccessPolicyRuleOfDeliveryGroup, True]}
Name                              : App Protection_AG
Uid                               : 37

AllowRestart                      : True
AllowedConnections                : NotViaAG
AllowedProtocols                  : {HDX, RDP}
AllowedUsers                      : AnyAuthenticated
AppProtectionKeyLoggingRequired   : False
AppProtectionScreenCaptureRequired : False
Description                       :
DesktopGroupName                  : App Protection
DesktopGroupUid                   : 15
Enabled                           : True
ExcludedClientIPFilterEnabled     : False
ExcludedClientIPs                 : {}
ExcludedClientNameFilterEnabled   : False
ExcludedClientNames               : {}
ExcludedSmartAccessFilterEnabled  : False
ExcludedSmartAccessTags           : {}
ExcludedUserFilterEnabled         : False
ExcludedUsers                     : {}
HdxSslEnabled                     : False
IncludedClientIPFilterEnabled     : False
IncludedClientIPs                 : {}
IncludedClientNameFilterEnabled   : False
IncludedClientNames               : {}
IncludedSmartAccessFilterEnabled  : True
IncludedSmartAccessTags           : {}
IncludedUserFilterEnabled         : True
IncludedUsers                     : {}
MetadataMap                       : {[IfBuiltInAccessPolicyRuleOfDeliveryGroup, True], [IfCreatedByOrchAccessPolicyRuleOfDeliveryGroup, True]}
Name                              : App Protection_Direct
Uid                               : 36
```

d) Obtenga las directivas que se aplican solo a un grupo de entrega en particular mediante el comando:

```
Get-BrokerAccessPolicyRule -DesktopGroupUid 7
```

e) Para filtrar los usuarios mediante dispositivos de confianza, cree otra directiva de acceso con intermediario mediante el comando:

```
New-BrokerAccessPolicyRule -Name CAP_Desktops_AG_Trusted-
DesktopGroupUid 7 - AllowedConnections ViaAG -AllowedProtocols
 HDX, RDP -AllowedUsers AnyAuthenticated - AllowRestart $true
 -Enabled $true-IncludedSmartAccessFilterEnabled $true
```

f) Para inhabilitar App Protection para dispositivos de confianza y habilitar App Protection para dispositivos que no son de confianza, utilice este comando:

```
Set-BrokerAccessPolicyRule CAP_Desktops_AG_trusted -IncludedSmartAcces
 Workspace:trusted -AppProtectionKeyLoggingRequired $false -
AppProtectionScreenCaptureRequired $false
```

```
Set-BrokerAccessPolicyRule CAP_Desktops_AG -IncludedSmartAccessTags
 Workspace:untrusted -AppProtectionKeyLoggingRequired $true -
AppProtectionScreenCaptureRequired $true
```

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

6. Verificación:

   Cierre sesión en la aplicación Citrix Workspace e iníciela de nuevo. Inicie el recurso protegido desde un dispositivo de confianza, uno que cumpla con la condición del análisis de EPA. Verá que las directivas de App Protection no se aplican. Inicie el mismo recurso desde un dispositivo que no sea de confianza. Verá que las directivas de App Protection se aplican.

Caso 3

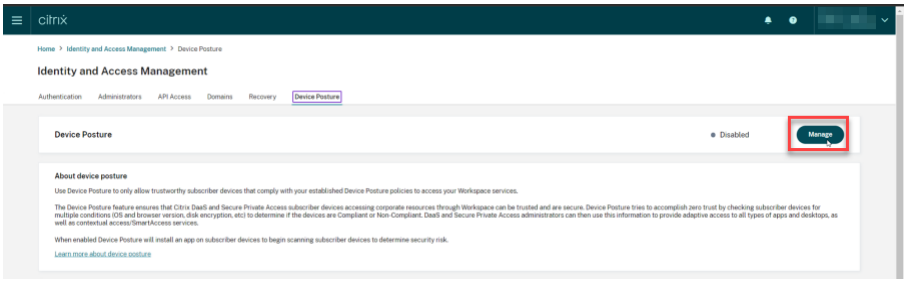
January 23, 2024

Este caso trata de cómo habilitar App Protection en función de los resultados de Device Posture.

1. Configurar Device Posture Service:

   a) Inicie sesión en Citrix Cloud.

   b) Vaya a **Administración de acceso e identidad** > **Device Posture** y haga clic en **Administrar**.



   c) Haga clic en **Crear directiva de dispositivos**.

      Aparece la página **Crear directiva de dispositivos**.

   d) En **Reglas de directiva**, haga clic en el menú desplegable **Seleccionar regla** y seleccione *Versión de la aplicación Citrix Workspace*.

   e) Haga clic en el menú desplegable **Seleccione una regla** y seleccione *Mayor o igual a* >=.

   f) Introduzca la versión de la aplicación Citrix Workspace que quiera establecer como condición. En este ejemplo, es *23.7.0.19*.

   g) En **Resultado de la directiva**, seleccione **Conforme**.

   h) En el campo **Nombre**, introduzca un nombre para la directiva.

   i) En el campo **Prioridad**, introduzca la prioridad de la directiva.

   j) Marque la casilla **Habilitar al crearla** para habilitar la directiva desde que la creó.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

k) Haga clic en **Crear**.

2. Configure las reglas de directivas de acceso con intermediario:

a) Instale el SDK de PowerShell para Citrix y conéctese a la API de la nube como se explica en el blog de Citrix Getting started with PowerShell automation for Citrix Cloud.

b) Ejecute el comando `Get-BrokerAccessPolicyRule`.

Se muestra una lista de todas las directivas de acceso con intermediario para todos los grupos de entrega presentes.

c) Busque el **DesktopGroupUid** del grupo de entrega que quiere cambiar.

```
PS C:\Windows\System32> Get-BrokerAccessPolicyRule


AllowRestart                      : True
AllowedConnections                : ViaAG
AllowedProtocols                  : {HDX, RDP}
AllowedUsers                      : AnyAuthenticated
AppProtectionKeyLoggingRequired   : False
AppProtectionScreenCaptureRequired : False
Description                       :
DesktopGroupName                  : App Protection
DesktopGroupUid                   : 15
Enabled                           : True
ExcludedClientIPFilterEnabled     : False
ExcludedClientIPs                 : {}
ExcludedClientNameFilterEnabled   : False
ExcludedClientNames               : {}
ExcludedSmartAccessFilterEnabled  : False
ExcludedSmartAccessTags           : {}
ExcludedUserFilterEnabled         : False
ExcludedUsers                     : {}
HdxSslEnabled                     : False
IncludedClientIPFilterEnabled     : False
IncludedClientIPs                 : {}
IncludedClientNameFilterEnabled   : False
IncludedClientNames               : {}
IncludedSmartAccessFilterEnabled  : True
IncludedSmartAccessTags           : {}
IncludedUserFilterEnabled         : True
IncludedUsers                     : {}
MetadataMap                       : {[IfBuiltInAccessPolicyRuleOfDeliveryGroup, True], [IfCreatedByOrchAccessPolicyRuleOfDeliveryGroup, True]}
Name                              : App Protection_AG
Uid                               : 37

AllowRestart                      : True
AllowedConnections                : NotViaAG
AllowedProtocols                  : {HDX, RDP}
AllowedUsers                      : AnyAuthenticated
AppProtectionKeyLoggingRequired   : False
AppProtectionScreenCaptureRequired : False
Description                       :
DesktopGroupName                  : App Protection
DesktopGroupUid                   : 15
Enabled                           : True
ExcludedClientIPFilterEnabled     : False
ExcludedClientIPs                 : {}
ExcludedClientNameFilterEnabled   : False
ExcludedClientNames               : {}
ExcludedSmartAccessFilterEnabled  : False
ExcludedSmartAccessTags           : {}
ExcludedUserFilterEnabled         : False
ExcludedUsers                     : {}
HdxSslEnabled                     : False
IncludedClientIPFilterEnabled     : False
IncludedClientIPs                 : {}
IncludedClientNameFilterEnabled   : False
IncludedClientNames               : {}
IncludedSmartAccessFilterEnabled  : True
IncludedSmartAccessTags           : {}
IncludedUserFilterEnabled         : True
IncludedUsers                     : {}
MetadataMap                       : {[IfBuiltInAccessPolicyRuleOfDeliveryGroup, True], [IfCreatedByOrchAccessPolicyRuleOfDeliveryGroup, True]}
Name                              : App Protection_Direct
Uid                               : 36
```

d) Obtenga las directivas que se aplican solo a un grupo de entrega en particular mediante el comando:

```
Get-BrokerAccessPolicyRule -DesktopGroupUid 7
```

e) Para aplicar App Protection a los dispositivos conformes, ejecute este comando:

```
Set-BrokerAccessPolicyRule "Contextual App Protection Delivery
 Group_AG"-IncludedSmartAccessFilterEnabled $true -IncludedSmartAccess
 Workspace:COMPLIANT
```

f) Para aplicar App Protection a los dispositivos no conformes, ejecute este comando:

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

```
New-BrokerAccessPolicyRule "Contextual App Protection Delivery
 Group_AG_NonCompliant"-DesktopGroupUid 7 -AllowedConnections
 ViaAG -AllowedProtocols HDX, RDP -Enabled $true -AllowRestart
 $true -ExcludedSmartAccessFilterEnabled $true -ExcludedSmartAccessTag
 Workspace:COMPLIANT-IncludedSmartAccessFilterEnabled $true
```

3. Verificación:

   Cierre sesión en la aplicación Citrix Workspace. Inicie sesión desde una versión de la aplicación Citrix Workspace conforme con la directiva de dispositivos. Verá que las directivas de App Protection no se aplican. De nuevo, cierre sesión en la aplicación Citrix Workspace e inicie sesión desde una versión de la aplicación Citrix Workspace que no esté conforme con la directiva de dispositivos. Verá que las directivas de App Protection se aplican.

Caso 4

October 27, 2023

En este caso, se explica cómo habilitar App Protection para grupos de usuarios específicos.

Estos pasos le permiten habilitar App Protection para los usuarios de un grupo específico:

1. Seleccione el grupo de usuarios de Active Directory para el que quiera habilitar las directivas de App Protection para los usuarios. En este ejemplo, el grupo de usuarios de Active Directory es **ProductManagers**.
2. Configure las reglas de directivas de acceso con intermediario:
   a) Instale el SDK de PowerShell para Citrix y conéctese a la API de la nube como se explica en el blog de Citrix Getting started with PowerShell automation for Citrix Cloud.
   b) Ejecute el comando `Get-BrokerAccessPolicyRule`.

      Se muestra una lista de todas las directivas de acceso con intermediario para todos los grupos de entrega presentes.
   c) Busque el **DesktopGroupUid** del grupo de entrega que quiere cambiar.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

```
PS C:\Windows\System32> Get-BrokerAccessPolicyRule


AllowRestart                      : True
AllowedConnections                : ViaAG
AllowedProtocols                  : {HDX, RDP}
AllowedUsers                      : AnyAuthenticated
AppProtectionKeyLoggingRequired   : False
AppProtectionScreenCaptureRequired : False
Description                       :
DesktopGroupName                  : App Protection
DesktopGroupUid                   : 15
Enabled                           : True
ExcludedClientIPFilterEnabled     : False
ExcludedClientIPs                 : {}
ExcludedClientNameFilterEnabled   : False
ExcludedClientNames               : {}
ExcludedSmartAccessFilterEnabled  : False
ExcludedSmartAccessTags           : {}
ExcludedUserFilterEnabled         : False
ExcludedUsers                     : {}
HdxSslEnabled                     : False
IncludedClientIPFilterEnabled     : False
IncludedClientIPs                 : {}
IncludedClientNameFilterEnabled   : False
IncludedClientNames               : {}
IncludedSmartAccessFilterEnabled  : True
IncludedSmartAccessTags           : {}
IncludedUserFilterEnabled         : True
IncludedUsers                     : {}
MetadataMap                       : {[IfBuiltInAccessPolicyRuleOfDeliveryGroup, True], [IfCreatedByOrchAccessPolicyRuleOfDeliveryGroup, True]}
Name                              : App Protection_AG
Uid                               : 37

AllowRestart                      : True
AllowedConnections                : NotViaAG
AllowedProtocols                  : {HDX, RDP}
AllowedUsers                      : AnyAuthenticated
AppProtectionKeyLoggingRequired   : False
AppProtectionScreenCaptureRequired : False
Description                       :
DesktopGroupName                  : App Protection
DesktopGroupUid                   : 15
Enabled                           : True
ExcludedClientIPFilterEnabled     : False
ExcludedClientIPs                 : {}
ExcludedClientNameFilterEnabled   : False
ExcludedClientNames               : {}
ExcludedSmartAccessFilterEnabled  : False
ExcludedSmartAccessTags           : {}
ExcludedUserFilterEnabled         : False
ExcludedUsers                     : {}
HdxSslEnabled                     : False
IncludedClientIPFilterEnabled     : False
IncludedClientIPs                 : {}
IncludedClientNameFilterEnabled   : False
IncludedClientNames               : {}
IncludedSmartAccessFilterEnabled  : True
IncludedSmartAccessTags           : {}
IncludedUserFilterEnabled         : True
IncludedUsers                     : {}
MetadataMap                       : {[IfBuiltInAccessPolicyRuleOfDeliveryGroup, True], [IfCreatedByOrchAccessPolicyRuleOfDeliveryGroup, True]}
Name                              : App Protection_Direct
Uid                               : 36
```

d) Obtenga las directivas que se aplican solo a un grupo de entrega en particular mediante el comando:

```
Get-BrokerAccessPolicyRule -DesktopGroupUid 7
```

e) Para habilitar directivas de App Protection para los usuarios del grupo de usuarios **ProductManagers**, ejecute estos comandos:

```
New-BrokerAccessPolicyRule "Example Rule Name_1"-DesktopGroupUid
 7 -AllowedConnections AnyViaAG -AllowedProtocols HDX -AllowedUsers
 Filtered -AppProtectionScreenCaptureRequired $true -IncludedUserFilte
 $true -IncludedUsers domain.com\ProductManagers
```

f) Para inhabilitar directivas de App Protection para los usuarios que no forman parte del grupo de usuarios **ProductManagers**, ejecute estos comandos:

```
New-BrokerAccessPolicyRule "Example Rule Name_2"-DesktopGroupUid
 7 -AllowedConnections AnyViaAG -AllowedProtocols HDX -AllowedUsers
 Filtered -AppProtectionScreenCaptureRequired $false-ExcludedUserFilte
 $true -ExcludedUsers domain.com\ProductManagers
```

3. Verificación:

Cierre la sesión de la aplicación Citrix Workspace si estaba abierta. Inicie sesión en la aplicación

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

Citrix Workspace como usuario del grupo de usuarios de Active Directory **ProductManagers**. Inicie el recurso protegido y podrá comprobar que App Protection está inhabilitada. Cierre sesión en la aplicación Citrix Workspace e inicie sesión de nuevo como un usuario que no forma parte del grupo de usuarios de Active Directory **ProductManagers**. Inicie el recurso protegido y verá que App Protection está habilitada.

Contextual App Protection para StoreFront

March 11, 2024

Contextual App Protection ofrece la posibilidad de aplicar directivas de App Protection de forma condicional a un subconjunto de usuarios, en función de sus características, sus dispositivos y la estrategia de red.

Implementar Contextual App Protection

Puede implementar Contextual App Protection por medio de los filtros de conexión definidos en la regla de directiva de acceso con intermediario. Las directivas de acceso con intermediario definen las reglas que controlan el acceso de un usuario a grupos de escritorios. La directiva comprende un conjunto de reglas. Cada regla se refiere a un único grupo de entrega y tiene un conjunto de filtros de conexión y controles de derechos de acceso.

Los usuarios pueden acceder a un grupo de entrega cuando los detalles de su conexión coinciden con los filtros de conexión de una o más reglas de la directiva de acceso con intermediario. De forma predeterminada, los usuarios no tienen acceso a ningún grupo de escritorios de un sitio. Puede crear más directivas de acceso con intermediario en función de sus requisitos. Se pueden aplicar varias reglas a un mismo grupo de entrega. Para obtener más información, consulte New-BrokerAccessPolicyRule.

Los siguientes parámetros de la regla de directiva de acceso con intermediario ofrecen la flexibilidad necesaria para habilitar App Protection en contexto si la conexión del usuario coincide con los filtros de conexión definidos en la regla de directiva de acceso:

- `AppProtectionKeyLoggingRequired`
- `AppProtectionScreenCaptureRequired`

Utilice los filtros de Smart Access a los que se hace referencia en las directivas de acceso con intermediario para precisar los filtros de conexión. Para obtener información sobre la configuración de filtros de Smart Access, consulte CTX227055. Para comprender cómo usar las directivas de Smart Access para configurar Contextual App Protection, consulte los casos siguientes.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

> **Nota:**
>
> Si App Protection está habilitada en el grupo de entrega, Contextual App Protection no se puede aplicar de forma predeterminada. Inhabilite App Protection en el grupo de entrega mediante este comando:
>
> ```
> Set-BrokerDesktopGroup -Name "Admin Desktop" -
>  AppProtectionKeyLoggingRequired $false -
>  AppProtectionScreenCaptureRequired $false
> <!--NeedCopy-->
> ```

Requisitos previos

Para habilitar Contextual App Protection para StoreFront, asegúrese de cumplir los requisitos mencionados en la sección Requisitos previos.

Habilitar Contextual App Protection

1. Descargue las directivas de Contextual App Protection (tabla de funciones) para su versión de Citrix Virtual Apps and Desktops desde la página Descargas de Citrix.
2. Ejecute este comando de PowerShell en el Delivery Controller:

   ```
   asnp Citrix*
   Set-BrokerSite -TrustRequestsSentToTheXmlServicePort $true
   <!--NeedCopy-->
   ```

3. Ejecute este comando para habilitar Contextual App Protection en el Delivery Controller:

   ```
   Import-ConfigFeatureTable <path to the downloaded feature table>
   <!--NeedCopy-->
   ```

   Por ejemplo:

   ```
   Import-ConfigFeatureTable\Downloads\FeatureTable.OnPrem.
      AppProtContextualAccess.xml
   <!--NeedCopy-->
   ```

Casos de Contextual App Protection

Estos son algunos de los casos sobre cómo puede habilitar o inhabilitar Contextual App Protection:

- Inhabilitar App Protection para ciertos tipos de dispositivos
- Inhabilitar App Protection para conexiones iniciadas desde acceso basado en explorador web y habilitar App Protection para conexiones desde la aplicación Citrix Workspace

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

- Inhabilitar App Protection para los usuarios de un grupo específico de Active Directory
- Habilitar App Protection para dispositivos en función de los resultados del análisis de EPA
- Habilitar App Protection para grupos de usuarios específicos

Requisitos previos

March 11, 2024

Asegúrese de tener lo siguiente:

- Citrix Virtual Apps and Desktops 2109 o una versión posterior
- Delivery Controller 2109 o una versión posterior
- StoreFront 1912 LTSR o una versión posterior
- Configuraciones de servidores virtual VPN o puertas de enlace y servidores virtuales de autenticación
- Una conexión correcta entre NetScaler y StoreFront. Para obtener más información, consulte Integrar NetScaler Gateway con StoreFront
- La importación de tablas XML es necesaria hasta la versión 2006 de Citrix Virtual Apps and Desktops
- La importación de tablas de la función de Contextual App Protection es necesaria hasta la versión 2209 de Citrix Virtual Apps and Desktops
- Habilite Smart Access en NetScaler Gateway para casos que requieran etiquetas Smart Access. Para obtener más información, consulte este artículo de asistencia.
- Requisitos del sistema de licencias:
  - Licencia local de App Protection
  - Licencia universal de Citrix Gateway para casos con etiquetas Smart Access

Caso 1

March 11, 2024

En este caso, se explica cómo inhabilitar App Protection para determinados tipos de dispositivos.

A continuación se muestran los pasos para inhabilitar App Protectionpara los usuarios de iPhone de un grupo de entrega llamado `Win10Desktop`:

1. Cree una directiva de Smart Access:

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

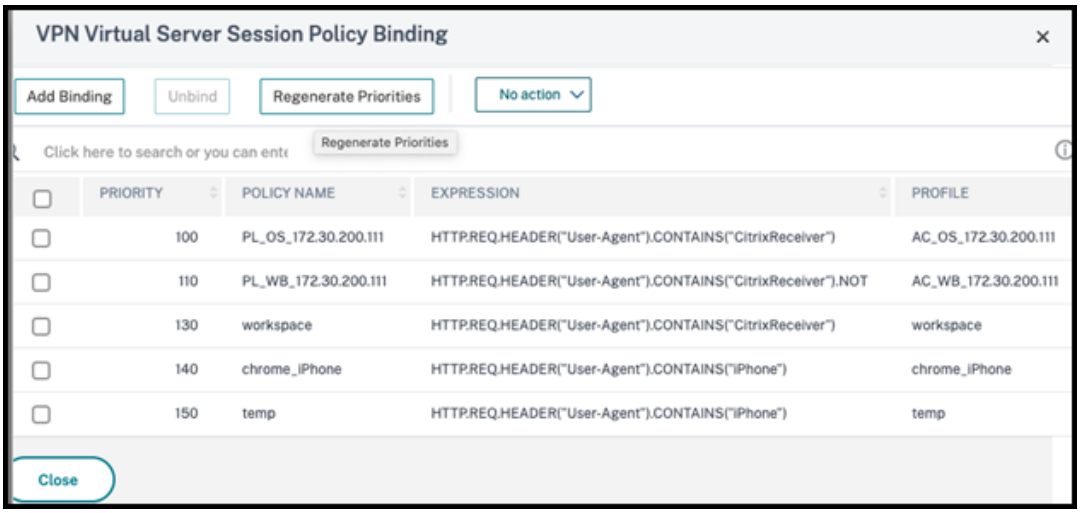
a) Inicie sesión en la interfaz de usuario de administración de Citrix ADC.

b) En el menú de navegación de la izquierda, vaya a **Citrix Gateway** > **Virtual Servers**.

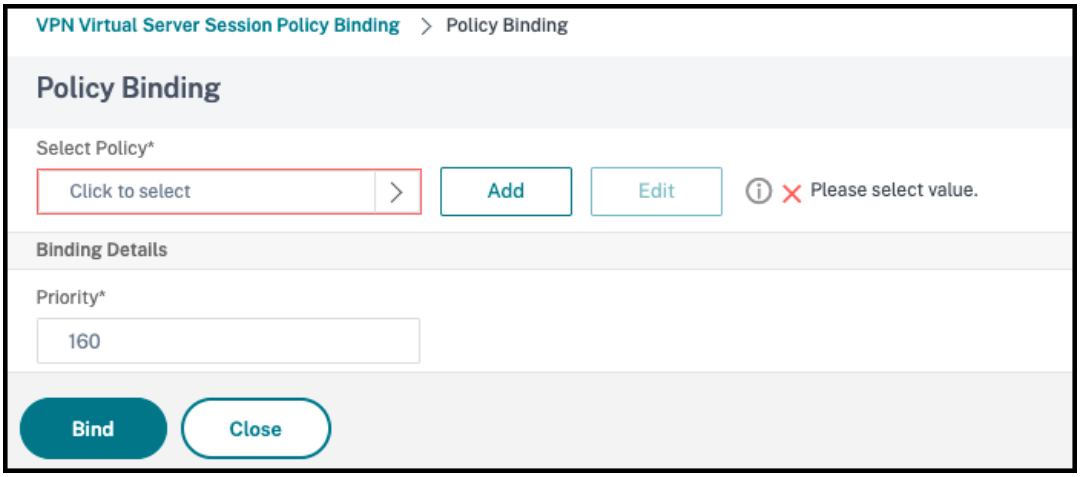
Anote el nombre del servidor virtual VPN, que se necesita para configurar la directiva de acceso con intermediario más adelante.

c) Haga clic en **VPN Virtual Server**. Desplácese a la sección inferior de la página y haga clic en **Session policies**. Aparece una lista de directivas de sesión.

d) Haga clic en **Add Binding**.

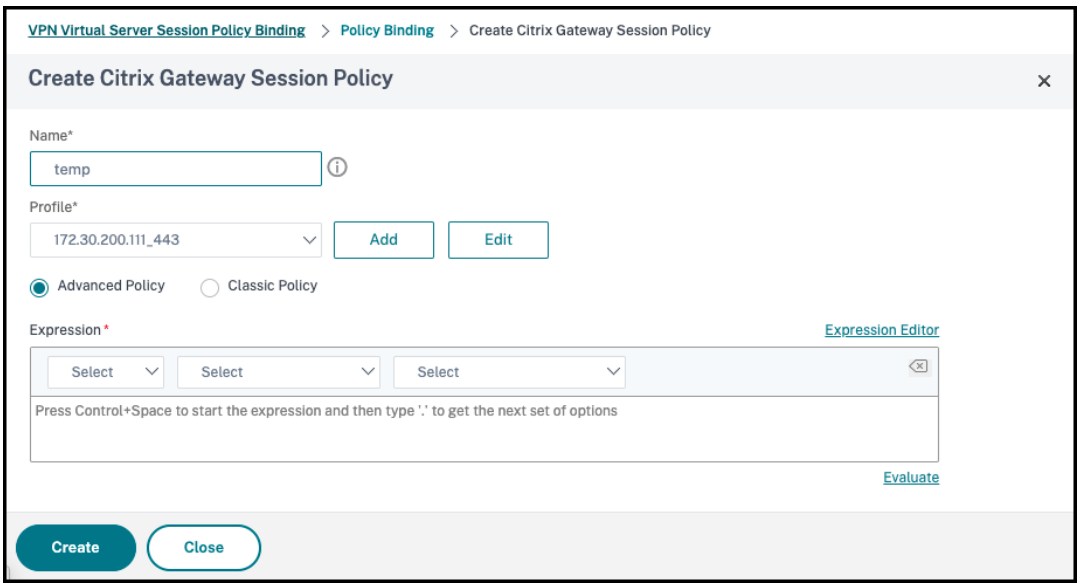


e) Haga clic en **Add to create a session policy**.

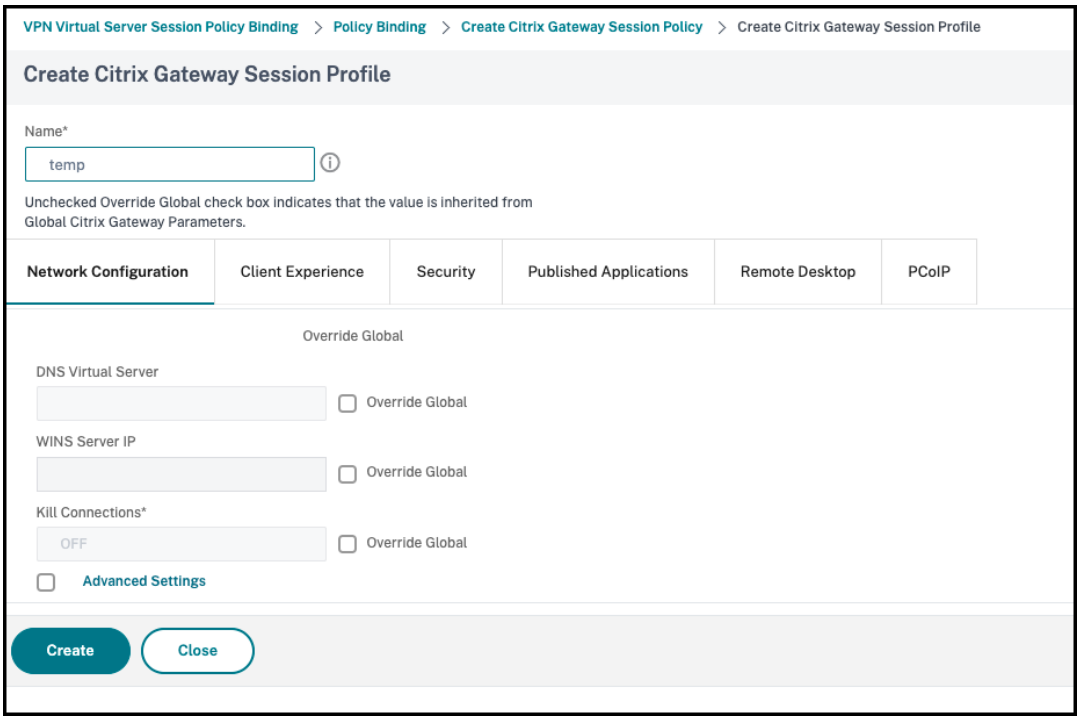


f) Introduzca un nombre para la directiva de sesión. En este caso, es *temp*.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.



g) Haga clic en **Add** junto a Profile para especificar un nombre de perfil. Haga clic en **Crear**.



h) Haga clic en **Expression Editor** en la ventana de directiva de sesión.

i) Cree esta expresión para comprobar si *iPhone* se halla en la cadena **User Agent**:

```
HTTP.REQ.HEADER("User-Agent").CONTAINS("iPhone")
<!--NeedCopy-->
```

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

j) Haga clic en **Bind** para crear la directiva de sesión.

2. Cree reglas de directiva de acceso con intermediario:

   Para aplicar la directiva a los usuarios de iPhone que acceden a `Win10Desktop` a través de Access Gateway, siga estos pasos:

   a) Ejecute este comando en el Delivery Controller (DDC):

```
Get-BrokerAccessPolicyRule
<!--NeedCopy-->
```

   Enumera todas las directivas de acceso con intermediario definidas en el DDC. En este caso, las directivas de acceso con intermediario para el grupo de entrega `Win10Desktop` son `Win10Desktop_AG` y `Win10Desktop_Direct`. Anote el UID del grupo de escritorios del grupo de entrega para el siguiente paso.

   b) Use este comando para crear una regla de directiva de acceso con intermediario para `Win10Desktop` a fin de filtrar los usuarios de iPhone que llegan a través de Access Gateway:

```
New-BrokerAccessPolicyRule -Name Win10Desktop_AG_iPhone -
    DesktopGroupUid <Uid_of_desktopGroup> -AllowedConnections
    ViaAG -AllowedProtocols HDX, RDP -AllowedUsers
    AnyAuthenticated -AllowRestart $true -
    AppProtectionKeyLoggingRequired $false -
    AppProtectionScreenCaptureRequired $false -Enabled $true -
    IncludedSmartAccessFilterEnabled $true
<!--NeedCopy-->
```

   Uid_of_desktopGroup es el UID del grupo de escritorios del grupo de entrega que se obtiene al ejecutar la regla GetBrokerAccessPolicy en el paso 1.

   c) Para inhabilitar App Protection para los usuarios de iPhone de `Win10Desktop` que llegan a través de Access Gateway, haga referencia a la etiqueta *temp* de Smart Access creada en el paso 1. Cree una directiva de Smart Access con este comando:

```
Set-BrokerAccessPolicyRule Win10Desktop_AG_iPhone -
    IncludedSmartAccessTags Primary_HDX_Proxy:temp -
```

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

```
    AppProtectionScreenCaptureRequired $false -
    AppProtectionKeyLoggingRequired $false
<!--NeedCopy-->
```

Primary_HDX_Proxy es el nombre del servidor virtual VPN del paso 1 anterior, Crear la directiva de Smart Access.

d) Para habilitar las directivas de App Protection para el resto de los usuarios de `Win10desktop`, use este comando:

```
Set-BrokerAccessPolicyRule Win10Desktop_AG -
    AppProtectionScreenCaptureRequired $true -
    AppProtectionKeyLoggingRequired $true
<!--NeedCopy-->
```

3. **Verificación**

   Para iPhones: Cierre la sesión de la aplicación Citrix Workspace si estaba abierta en el iPhone. Inicie sesión en la aplicación Citrix Workspace de forma externa a través de una conexión de Access Gateway. Puede ver los recursos necesarios en StoreFront, y App Protection debe estar inhabilitada.

   Para dispositivos que no sean iPhone: Cierre sesión en la aplicación Citrix Workspace si estaba abierta en el dispositivo. Inicie sesión en la aplicación Citrix Workspace de forma externa a través de una conexión de Access Gateway. Puede ver los recursos necesarios en StoreFront, y App Protection debe estar inhabilitado.

Caso 2

March 11, 2024

Este caso trata de cómo inhabilitar App Protection para conexiones iniciadas con acceso mediante explorador web y cómo habilitarla para conexiones desde la aplicación Citrix Workspace.

Estos son los pasos para inhabilitar App Protection para un grupo de entrega llamado `Win10Desktop` cuando las conexiones se inician desde un explorador web y cómo habilitar App Protection para las conexiones procedentes de la aplicación Citrix Workspace:

1. Cree directivas de Smart Access:

   a) Cree una directiva de Smart Access para filtrar las conexiones iniciadas desde la aplicación Citrix Workspace, tal y como se definió en el caso anterior, **Inhabilitar App Protection para determinados tipos de dispositivos**. Cree esta expresión para comprobar si **CitrixReceiver** se halla en la cadena **User Agent**:

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

```
HTTP.REQ.HEADER("User-Agent").CONTAINS("CitrixReceiver")
<!--NeedCopy-->
```

En este caso, la directiva de Smart Access es `cwa`.

b) Cree otra directiva de Smart Access para filtrar las conexiones que no se inician desde la aplicación Citrix Workspace, `HTTP.REQ.HEADER("User-Agent").CONTAINS("CitrixReceiver").NOT`. En este caso, la directiva de Smart Access es *browser*.

2. Cree reglas de directiva de acceso con intermediario:

a) Ejecute `GetBrokerAccessPolicyRule` para ver las dos directivas de acceso con intermediario para `Win10Desktop`. Para el grupo de entrega `Win10Desktop`, las directivas de acceso con intermediario son `Win10Desktop_AG` y `Win10Desktop_Direct`. Anote el UID del grupo de escritorios de `Win10Desktop`.

b) Cree una directiva de acceso con intermediario para `Win10Desktop` a fin de filtrar conexiones iniciadas desde la aplicación Citrix Workspace mediante este comando:

```
New-BrokerAccessPolicyRule -Name Win10Desktop_AG_CWA -
    DesktopGroupUid <Uid_of_desktopGroup> -AllowedConnections
    ViaAG -AllowedProtocols HDX, RDP -AllowedUsers
    AnyAuthenticated -AllowRestart $true -Enabled $true -
    IncludedSmartAccessFilterEnabled $true
<!--NeedCopy-->
```

Uid_of_desktopGroup es el UID del grupo de escritorios del grupo de entrega que se obtiene al ejecutar la regla GetBrokerAccessPolicy en el paso 1.

c) Use este comando para habilitar las directivas de App Protection solo en aquellas conexiones que llegan a través de CWA mediante una referencia a la etiqueta de Smart Access `cwa`:

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

```
Set-BrokerAccessPolicyRule Win10Desktop_AG_CWA -
    IncludedSmartAccessTags Primary_HDX_Proxy:cwa -
    AppProtectionScreenCaptureRequired $true -
    AppProtectionKeyLoggingRequired $true
<!--NeedCopy-->
```

Primary_HDX_Proxy es el nombre del servidor virtual VPN anotado anteriormente en el paso 1, Crear directiva de Smart Access.

d) Use este comando para inhabilitar las directivas de App Protection para el resto de las conexiones que llegan a través del explorador web:

```
Set-BrokerAccessPolicyRule Win10Desktop_AG -
    IncludedSmartAccessTags Primary_HDX_Proxy:browser -
    AppProtectionScreenCaptureRequired $false -
    AppProtectionKeyLoggingRequired $false
<!--NeedCopy-->
```

3. **Verificación**

   Cierre la sesión de la aplicación Citrix Workspace si estaba abierta. Inicie sesión de nuevo en la aplicación Citrix Workspace e inicie el recurso necesario desde una conexión externa a través de Access Gateway. Podrá ver que las directivas de App Protection están habilitadas para el recurso. Inicie el mismo recurso desde el explorador web a través de una conexión externa y podrá ver que las directivas de App Protection están inhabilitadas.

Caso 3

March 11, 2024

Este caso trata de cómo inhabilitar App Protection para los usuarios de un grupo específico de Active Directory.

Estos pasos sirven para inhabilitar App Protection para usuarios de `Win10Desktop` que forman parte del grupo de Active Directory **xd.local\sales**:

1. Ejecute `Get-BrokerAccessPolicyRule` para ver las dos directivas de acceso con intermediario para `Win10Desktop`. Para un grupo de entrega `Win10Desktop` hay dos directivas de acceso con intermediario `Win10Desktop_AG` y `Win10Desktop_Direct`. Anote el UID del grupo de escritorios del `Win10Desktop`.
2. Cree una regla de directiva de acceso con intermediario para `Win10Desktop` a fin de filtrar las conexiones de los usuarios del grupo de Active Directory `xd.local\sales`.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

```
New-BrokerAccessPolicyRule -Name Win10Desktop_AG_Sales_Group -
    DesktopGroupUid <Uid_of_desktopGroup> -AllowedConnections ViaAG
     -AllowedProtocols HDX, RDP -AllowedUsers Filtered -
    AllowRestart $true -Enabled $true
<!--NeedCopy-->
```

Uid_of_desktopGroup es el UID del grupo de escritorios del grupo de entrega que se obtiene al ejecutar la regla GetBrokerAccessPolicy en el paso 1.

3. Use este comando para inhabilitar las directivas de App Protection para los usuarios de Win10Desktop que forman parte del grupo de AD **xd.local\sales**:

```
Set-BrokerAccessPolicyRule Win10Desktop_AG_Sales_Group -
    AllowedUsers Filtered -IncludedUsers xd.local\sales -
    IncludedUserFilterEnabled $true -
    AppProtectionScreenCaptureRequired $false -
    AppProtectionKeyLoggingRequired $false
<!--NeedCopy-->
```

4. Use este comando para habilitar las directivas de App Protection para el resto de las conexiones de puerta de enlace, excepto para los usuarios de **xd.local\sales**:

```
Set-BrokerAccessPolicyRule Win10Desktop_AG -AllowedUsers
    Anyauthenticated -ExcludedUserFilterEnabled $true -
    ExcludedUsers xd.local\sales -
    AppProtectionScreenCaptureRequired $true -
    AppProtectionKeyLoggingRequired $true
<!--NeedCopy-->
```

5. **Verificación**

   Cierre la sesión de la aplicación Citrix Workspace si estaba abierta. Inicie sesión en la aplicación Citrix Workspace como usuario del grupo de Active Directory **xd.local\sales**. Inicie el recurso protegido y podrá comprobar que App Protection está inhabilitada.

   Cierre sesión en la aplicación Citrix Workspace e inicie sesión de nuevo como usuario que no forma parte de **xd.local\sales**. Inicie el recurso protegido y verá que App Protection está habilitada.

Caso 4

March 11, 2024

Este caso trata de cómo habilitar App Protection para dispositivos en función de los resultados del análisis de EPA.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

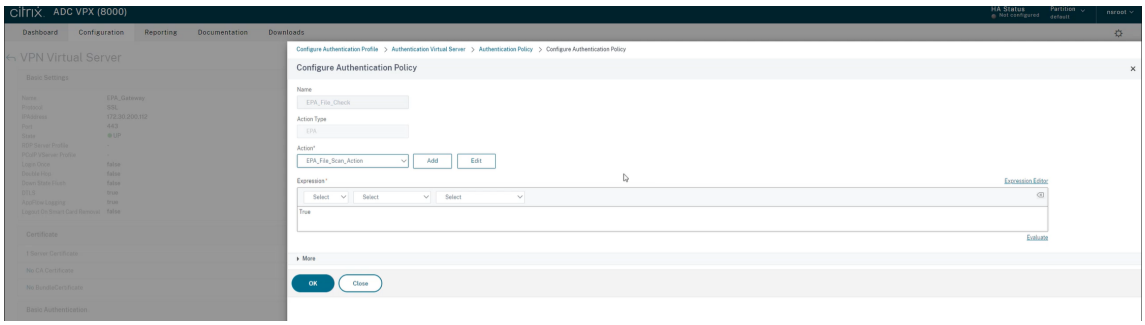
Estos pasos describen cómo habilitar App Protection para los dispositivos que superan los análisis de la EPA:

Requisitos previos:

Asegúrese de tener lo siguiente:

- Autenticación, autorización y auditoría de grupos de usuarios (para grupos de usuarios predeterminados y en cuarentena) y directivas asociadas
- Configuraciones de servidores de LDAP y directivas asociadas

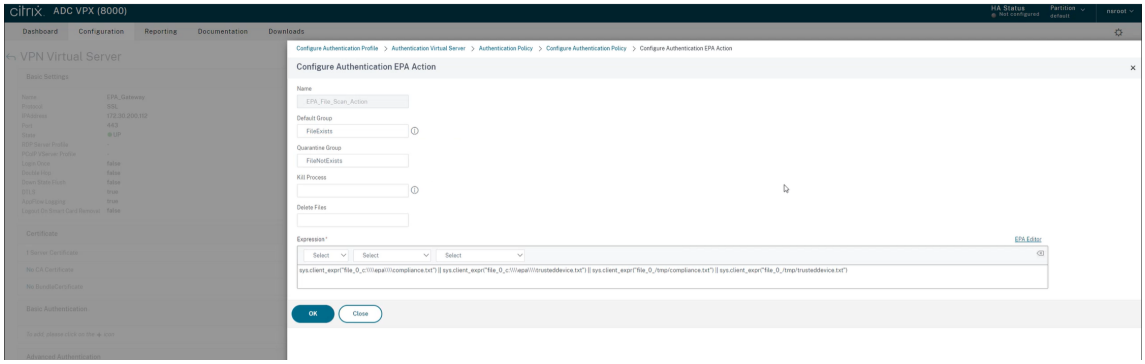
1. Inicie sesión en Citrix ADC y vaya a **Configuration** > **Citrix Gateway** > **Virtual Servers**.
2. Seleccione el servidor virtual correspondiente y haga clic en **Edit**.
3. Modifique el perfil de autenticación existente.
4. Seleccione el servidor virtual correspondiente y haga clic en **Edit**.
5. Haga clic en **Authentication Policies** > **Add Binding**.
6. En **Select Policy**, haga clic en **Add**.
7. En el campo **Name**, introduzca el nombre de la directiva de autenticación.
8. En la lista desplegable **Action Type**, seleccione **EPA**.
9. En el campo **Expression**, introduzca `True`.



10. En **Action**, haga clic en **Add**.
11. En el campo **Name**, introduzca el nombre de la acción de EPA.
12. Introduzca los nombres de **Default Group** y **Quarantine Group**. En este caso, el nombre de **Default Group** es **FileExists**, y el nombre de **Quarantine Group** es **FileNotExists**.
13. En el campo **Expression**, introduzca este valor:

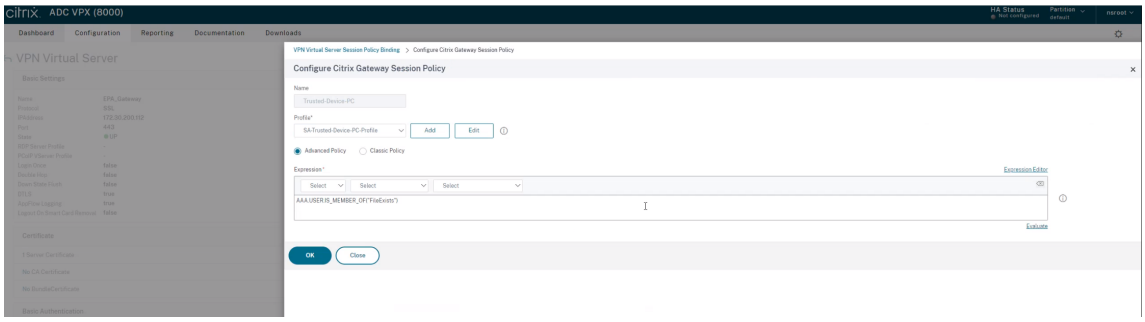
```
sys.client_expr("file_0_c:\\epa\\compliance.txt") || sys.
    client_expr("file_0_c:\\epa\\trusteddevice.txt") || sys.
    client_expr("file_0_/tmp/compliance.txt") || sys.client_expr("
    file_0_/tmp/trusteddevice.txt")
<!--NeedCopy-->
```

© 1999–2024 Cloud Software Group, Inc. All rights reserved.



14. Haga clic en **Create** y, a continuación, en **Bind**.
15. Haga clic en **Session Policies** > **Add Binding**.
16. En **Select Policy**, haga clic en **Add**.
17. En el campo **Name**, introduzca el nombre de la directiva de sesión.
18. En el campo **Expression**, introduzca este valor:

```
AAA.USER.IS_MEMBER_OF("FileExists")
<!--NeedCopy-->
```



19. Haga clic en **Create** y, a continuación, en **Bind**.
20. En el extremo izquierdo de la barra de tareas, haga clic en el icono **Buscar** .
21. Escriba **PowerShell** y abra **Windows PowerShell**.
22. Use este comando para inhabilitar las directivas de App Protection para los dispositivos que hayan superado los análisis de EPA mediante una referencia a la **etiqueta de Smart Access "EPA_GW:Trusted-Device-PC"**:

```
Set-BrokerAccessPolicyRule "Contextual App Protection Delivery
    Group_AG" -IncludedSmartAccessFilterEnabled $true -
    IncludedSmartAccessTags EPA_GW:Trusted-Device-PC -
    AppProtectionScreenCaptureRequired $false
<!--NeedCopy-->
```

Donde *EPA_GW* es el nombre del servidor virtual VPN.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

23. Use este comando para habilitar las directivas de App Protection para los dispositivos que no hayan superado los análisis de EPA mediante una referencia a la **etiqueta de Smart Access "EPA_GW:Trusted-Device-PC":**

```
1 New-BrokerAccessPolicyRule "Contextual App Protection Delivery
     Group_AG_NonCompliant"-DesktopGroupUid 17 -AllowedConnections
     ViaAG -AllowedProtocols HDX, RDP -Enabled $true -AllowRestart
     $true -ExcludedSmartAccessFilterEnabled $true -
     ExcludedSmartAccessTags EPA_GW:Trusted-Device-PC -
     IncludedSmartAccessFilterEnabled $true -
     AppProtectionScreenCaptureRequired $true
2 <!--NeedCopy-->
```

24. **Verificación**

    Cierre la sesión de la aplicación Citrix Workspace si estaba abierta. Inicie sesión en la aplicación Citrix Workspace desde un dispositivo de confianza. Inicie el recurso protegido y podrá comprobar que App Protection está inhabilitada.

    Cierre sesión en la aplicación Citrix Workspace e iníciela de nueva desde un dispositivo que no sea de confianza. Inicie el recurso protegido y verá que App Protection está habilitada.

Caso 5

November 28, 2023

En este caso, se explica cómo habilitar App Protection para grupos de usuarios específicos.

Para habilitar App Protection para los usuarios de un grupo específico, consulte Habilitar App Protection para grupos de usuarios específicos.

Compatibilidad de App Protection con el inicio híbrido a través de Workspace

March 11, 2024

Los inicios híbridos de Citrix Virtual Apps and Desktops tienen lugar al iniciar sesión en Citrix Workspace para Web al escribir la URL del almacén en el explorador nativo e iniciar las aplicaciones y escritorios virtuales a través de la aplicación Citrix Workspace nativa y su motor HDX. El término híbrido hace referencia al uso combinado de la aplicación Citrix Workspace para Web y la aplicación Citrix Workspace nativa para conectar y usar los recursos.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

> **Nota:**
>
> Si no hay ningún componente nativo de la aplicación Citrix Workspace instalado en el dispositivo de punto final, se trata de una configuración Zero Install en la que tanto el almacén de Citrix Workspace como el motor HDX están dentro del explorador web. Este caso se denomina aplicación Citrix Workspace para HTML5, que está alojada en Citrix Workspace o Citrix StoreFront. En este documento no se aborda ese supuesto.

Requisitos previos

- Asegúrese de usar un explorador que admita la extensión web de Citrix Workspace.
- Asegúrese de que el sufijo DNS de la URL de Workspace es cloud.com. Actualmente, no se admiten los dominios personalizados.
- Asegúrese de utilizar una de estas versiones de la aplicación Citrix Workspace:
  - Aplicación Citrix Workspace para Windows 2106 o una versión posterior
  - Aplicación Citrix Workspace para macOS 2106 o una versión posterior

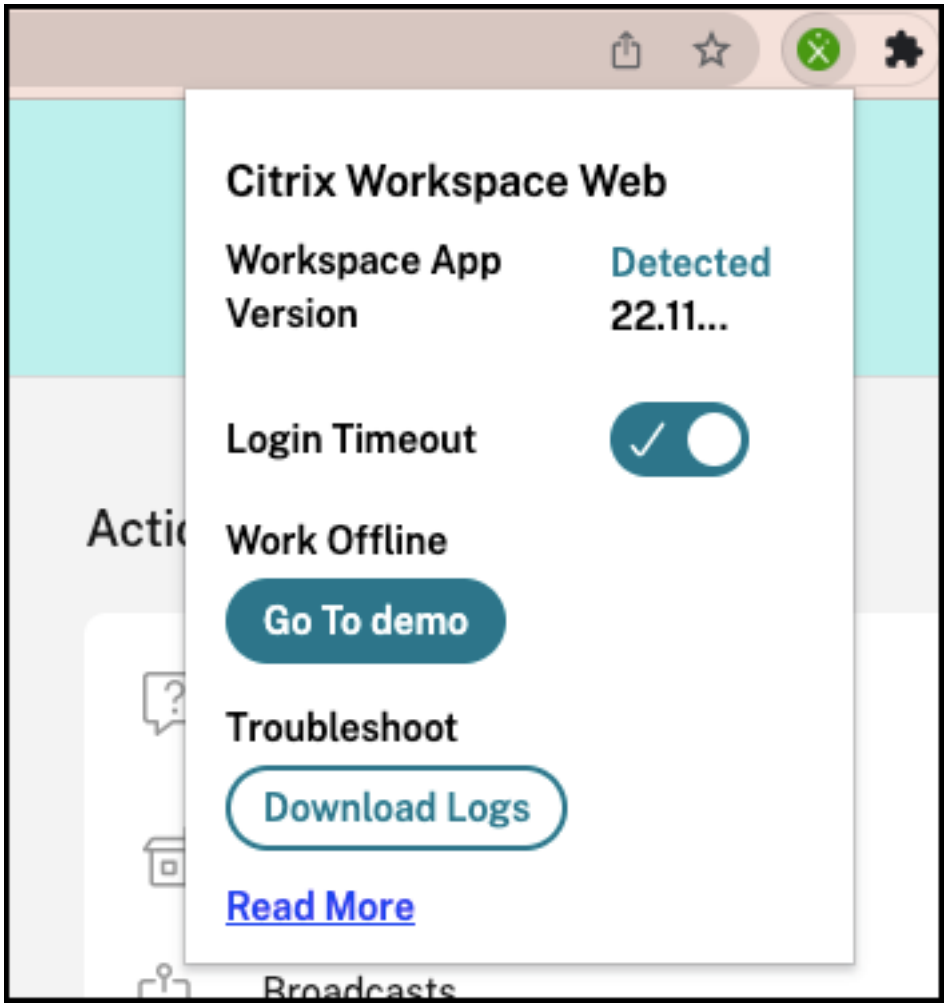
Habilite App Protection para el inicio híbrido

1. Instale la extensión web de Citrix Workspace en su explorador antes de agregar el almacén. Utilice uno de los siguientes enlaces en función de su explorador web:

   - Chrome
   - Edge Chromium

   Una vez que instale la extensión, se mostrará en la sección de extensiones del explorador.

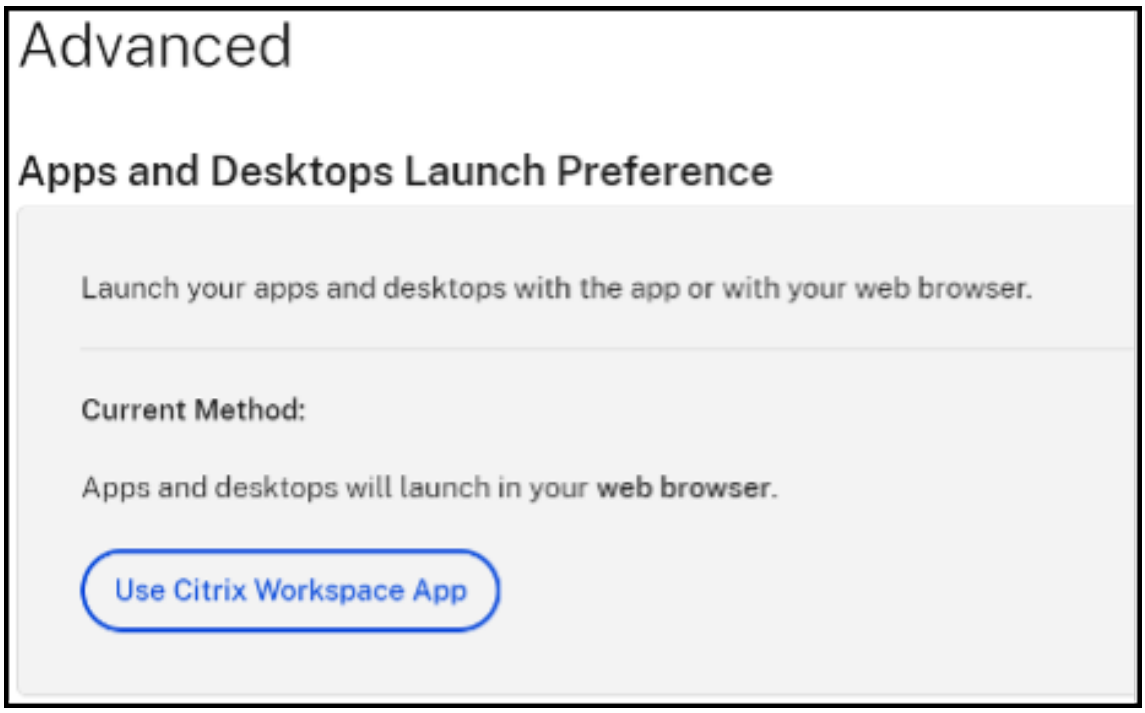
© 1999–2024 Cloud Software Group, Inc. All rights reserved.



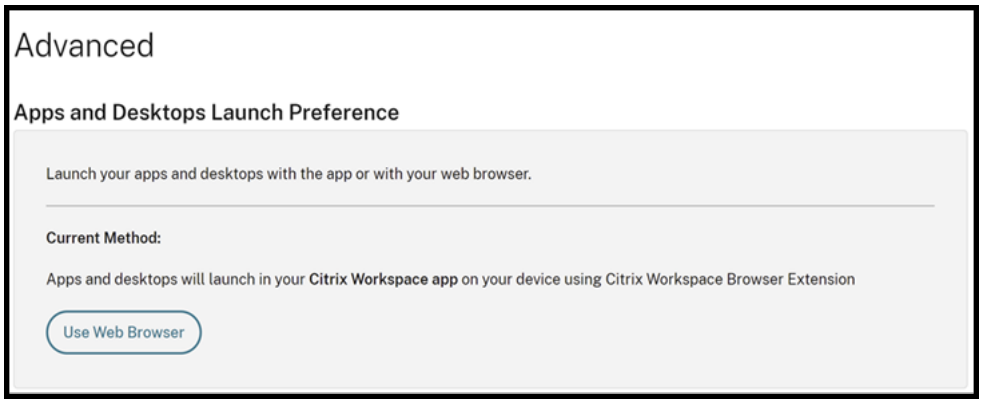
2. Inicie sesión en el almacén desde su explorador nativo.
3. Vaya a su **Perfil > Parámetros de cuenta > Avanzados**.

   En la sección **Preferencia de inicio de aplicaciones y escritorios**, puede ver el método con el que las aplicaciones y los escritorios se inician actualmente en su explorador web. Haga clic en **Usar la aplicación Citrix Workspace**.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.



Si utiliza la aplicación Citrix Workspace para iniciar los recursos, verá la siguiente opción. En tal caso, no se requieren cambios.



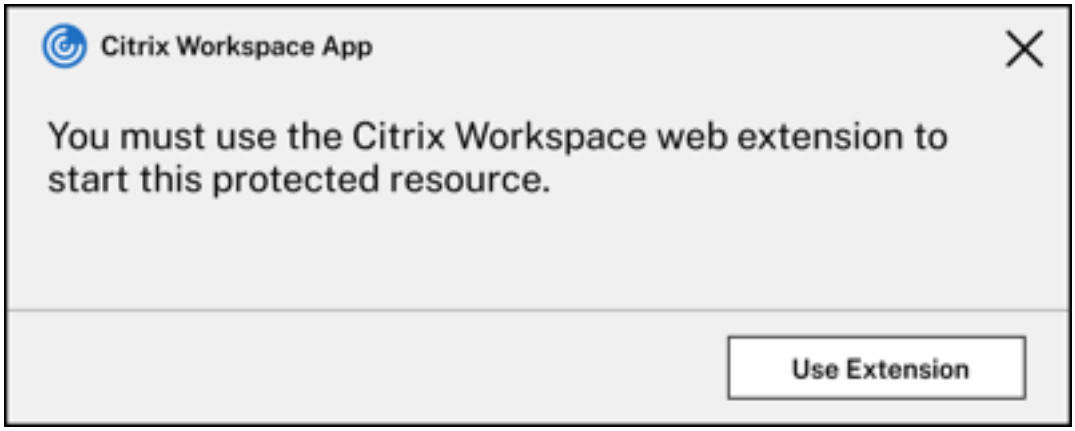
4. Ahora puede iniciar su aplicación o escritorio virtual protegidos.

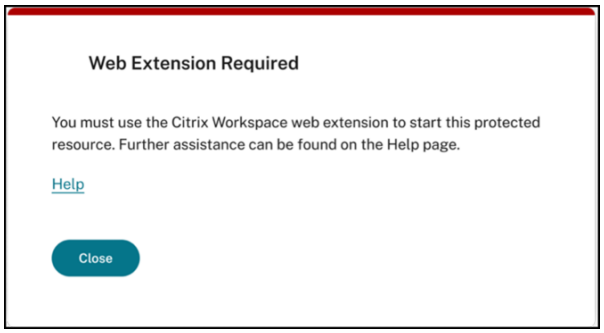
Escenarios de fallo comunes

A continuación, se muestran algunos casos de errores en el inicio y cómo solucionarlos.

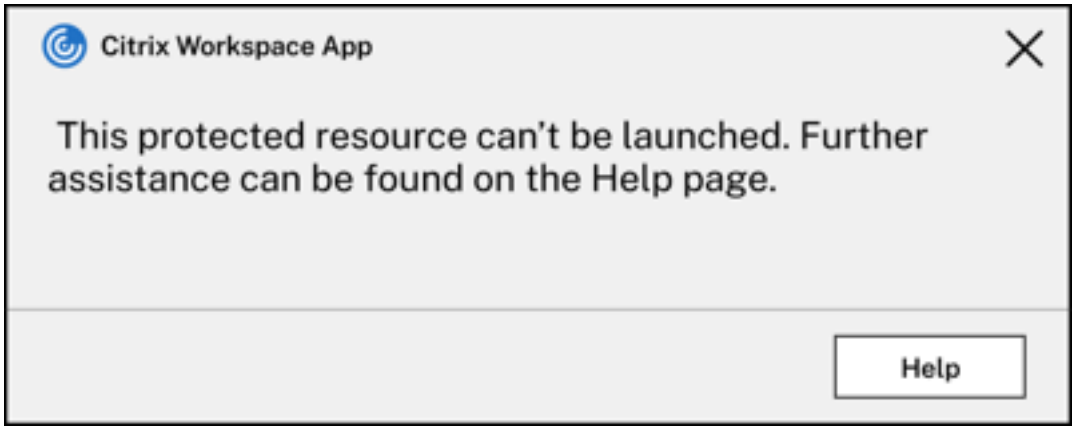
- Al inhabilitar o desinstalar la extensión web de Citrix Workspace antes de iniciar la aplicación protegida, aparece uno de los siguientes errores. Para evitarlo, instale la extensión antes de iniciar sesión en Citrix Workspace para Web.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

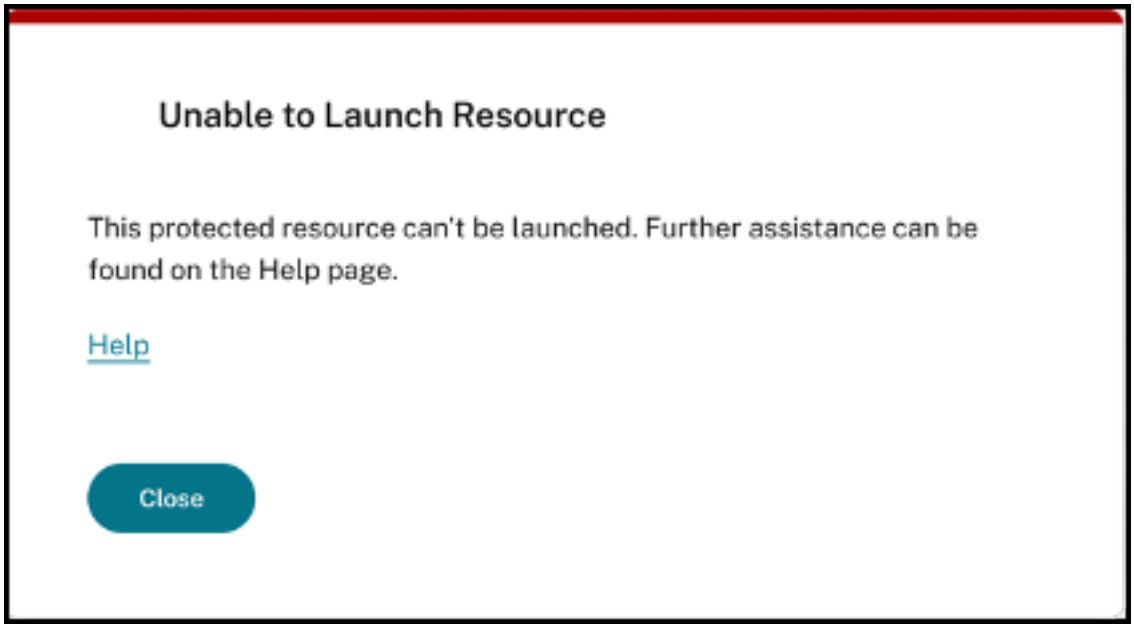




- Se produce uno de los siguientes errores cuando la preferencia de inicio está establecida como **Explorador Web**. Cambie la preferencia de inicio a **Usar la aplicación Citrix Workspace** para resolver este error. Para obtener más información, consulte este artículo de asistencia.



© 1999–2024 Cloud Software Group, Inc. All rights reserved.



Compatibilidad de App Protection con el inicio híbrido a través de StoreFront

March 11, 2024

El inicio híbrido de Citrix Virtual Apps and Desktops tiene lugar al iniciar sesión en StoreFront para Web tras introducir la URL del almacén en el explorador web nativo e iniciar las aplicaciones y escritorios virtuales a través de la aplicación Citrix Workspace nativa y su motor HDX. El término híbrido hace referencia al uso combinado de la aplicación StoreFront para Web y la aplicación Citrix Workspace nativa para conectar y usar los recursos.

> **Nota:**
>
> Si no hay ningún componente nativo de la aplicación Citrix Workspace instalado en el dispositivo de punto final, se trata de una configuración Zero Install en la que tanto el almacén de Citrix Workspace como el motor HDX están dentro del explorador web. Este caso se denomina aplicación Citrix Workspace para HTML5, que está alojada en Citrix Workspace o Citrix StoreFront. En este documento no se aborda ese supuesto.

La compatibilidad de App Protection para el inicio híbrido a través de StoreFront permite mostrar y ejecutar recursos habilitados con App Protection desde exploradores web.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

> **Nota:**
>
> Si selecciona las opciones **Usar versión simplificada** (que utiliza el cliente HTML5) o **Ya instalado**, las sesiones habilitadas para la App Protection se bloquean, puesto que la aplicación Citrix Workspace no se detecta correctamente en el explorador web.

Si utiliza StoreFront 2308 o una versión posterior, puede acceder a las aplicaciones y escritorios que tienen habilitadas directivas de App Protection mediante un explorador web si StoreFront está configurado adecuadamente y el explorador web detecta correctamente la aplicación Citrix Workspace nativa. Si usa versiones de StoreFront entre 1912 y 2203, debe aplicar la personalización tal y como se describe en la sección Cómo implementar.

> **Limitación:**
>
> StoreFront determina la versión de la aplicación Citrix Workspace al iniciar sesión en el sitio web por primera vez. Si más tarde instala una versión diferente de la aplicación Citrix Workspace, StoreFront no se da cuenta del cambio. Por lo tanto, es posible que permita o impida incorrectamente el inicio de aplicaciones y escritorios virtuales habilitados con directivas de App Protection. Citrix recomienda configurar la comprobación de la postura de App Protection, que bloquea el inicio de Virtual Apps and Desktops desde versiones anteriores de la aplicación Citrix Workspace que no presenten compatibilidad con App Protection. Para obtener más información sobre la verificación de la postura, consulte Verificación de la postura de App Protection.

Inicio híbrido a través de StoreFront, versión 2308 o una posterior

La versión 2308 y versiones posteriores de StoreFront son compatibles automáticamente con el inicio híbrido de aplicaciones y escritorios virtuales habilitados con directivas de App Protection. Para obtener más información sobre cómo habilitar App Protection para el inicio híbrido en StoreFront 2308 o versiones posteriores, consulte App Protection para el inicio híbrido a través de StoreFront.

Inicio híbrido a través de las versiones de StoreFront entre 1912 y 2203

Las versiones de StoreFront entre 1912 y 2203 son compatibles con el inicio híbrido de aplicaciones y escritorios virtuales que están habilitados con directivas de App Protection mediante esta personalización:

Citrix recomienda quitar esta personalización al actualizar StoreFront a la versión 2308 o una posterior.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

Requisitos previos

Para obtener información sobre las versiones necesarias de los componentes de Citrix para App Protection, consulte Requisitos del sistema.

Cómo implementar

1. Descargue el archivo ZIP *stf-customization-AppP.zip*, que contiene todos los archivos necesarios que debe implementar en la máquina de servidor de StoreFront. Descargue el archivo desde la página Descargas de Citrix. El archivo incluye lo siguiente:

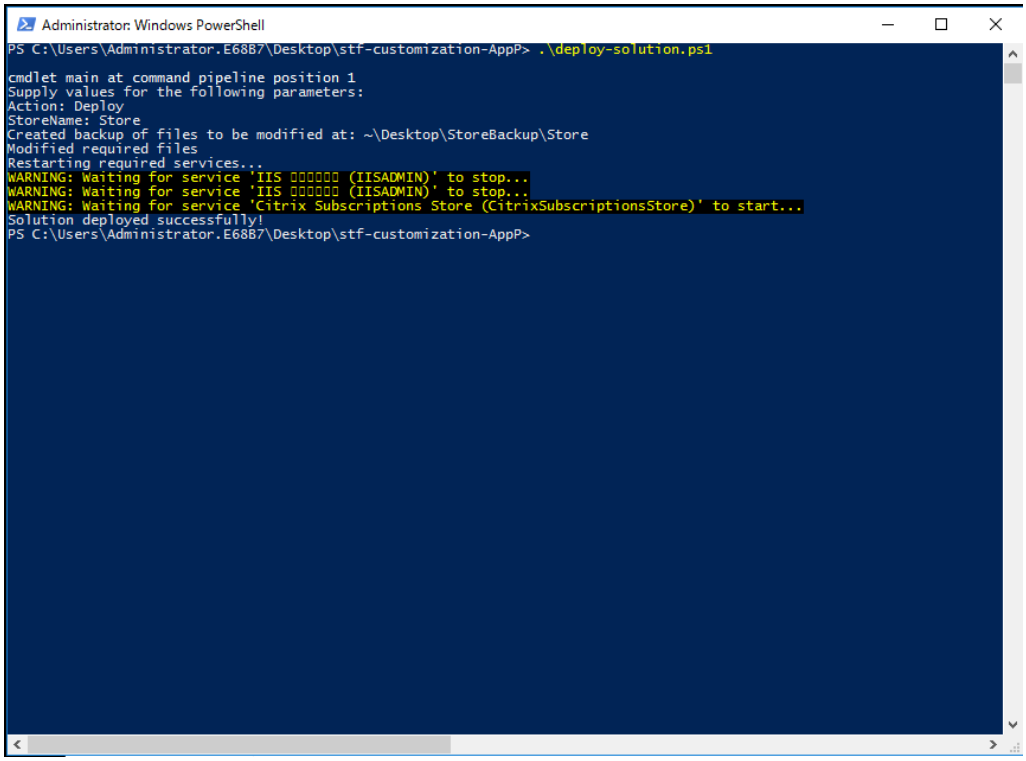
   - DLL que deben copiarse en la carpeta "bin"del almacén
   - Archivos JavaScript y otros archivos necesarios para que la solución funcione
   - Script de PowerShell*deploy-solution.ps1*, que el administrador de StoreFront utiliza para implementar la solución

2. Descomprima el archivo *stf-customization-AppP.zip* y abra un nuevo símbolo del sistema de PowerShell del administrador en la ubicación donde se extraerán los archivos. Ejecute el comando `deploy-solution.ps1`, que toma estos argumentos:

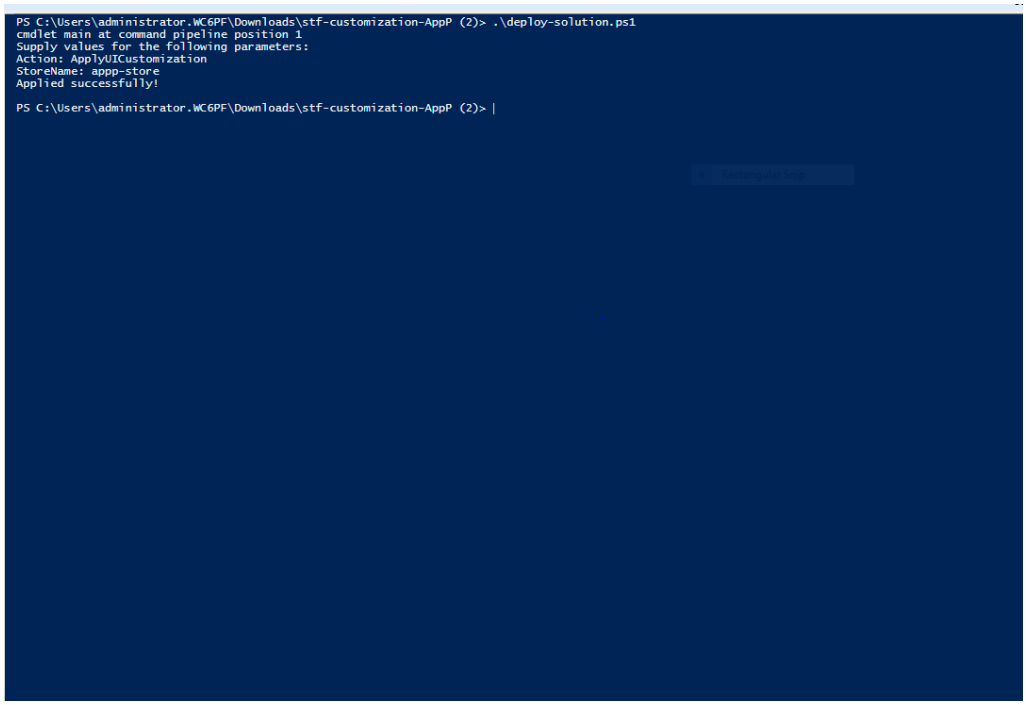
   - `-Action`: La acción que realiza el script. Los valores permitidos son los siguientes:

     - La acción `Deploy` implementa la solución de una manera fluida. Crea una copia de seguridad de los archivos que esta solución cambia, copia los archivos de la solución y reinicia los servicios. La siguiente captura de pantalla describe el comando para implementar la solución en el servidor de StoreFront:

© 1999–2024 Cloud Software Group, Inc. All rights reserved.



- La acción `ApplyUICustomization` personaliza la interfaz de usuario del almacén para que no se vean las opciones **Ya instalado** y **Usar versión simplificada**. Esta acción fuerza la detección de la aplicación Citrix Workspace nativa en el explorador web y garantiza que se omitan los casos bloqueados o no compatibles.



- La acción `RemoveUICustomization` deshace la acción de `ApplyUICustomization`

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

y las opciones **Ya instalado** y **Usar versión simplificada** se muestran de nuevo.

- `-StoreName`: Nombre del almacén para el que se debe realizar la acción. Este parámetro es obligatorio y debe transmitirse junto con la acción `Deploy`.
- `-BackupDir`: Parámetro que se puede incluir con la acción `Deploy` para crear una copia de seguridad en el directorio requerido. Si no se incluye, la copia de seguridad se crea en el escritorio. Este parámetro es un parámetro opcional.

> **Nota:**
>
> Si ya hay personalizaciones en *StoreCustomization_Input.dll* o *StoreCustomization_Launch.dll*, la implementación de esta solución las anula.

Las aplicaciones y escritorios habilitados para App Protection solo se enumerarán después de implementar las personalizaciones. Sin la implementación, las aplicaciones y los escritorios no se muestran.

Cómo revertir la personalización de StoreFront

Realice los siguientes pasos para revertir la personalización anterior de StoreFront:

1. Vaya al directorio *\Escritorio\StoreBackup<store name>* y copie los siguientes archivos en los directorios correspondientes:
   - Los archivos *StoreCustomization_Input.dll* y *StoreCustomization_Launch.dll* en el directorio *IISINETPub\Citrix<store name>\bin*
   - El archivo *web.config* en el directorio *IISINETPub\Citrix\StoreWeb*
   - Los archivos **.js* y *style.css* en el directorio *IISINETPub\Citrix\StoreWeb\Custom*

     > **Nota:**
     >
     > Si hay archivos de personalización distintos de los archivos anteriores en el directorio \Escritorio\StoreBackup<store name>, cópielos en los directorios pertinentes según convenga.

2. Abra PowerShell.
3. Detenga los servicios **IISADMIN** y **CitrixSubscriptionsStore** ejecutando los siguientes comandos:

```
sc stop IISADMIN
sc stop CitrixSubscriptionsStore
<!--NeedCopy-->
```

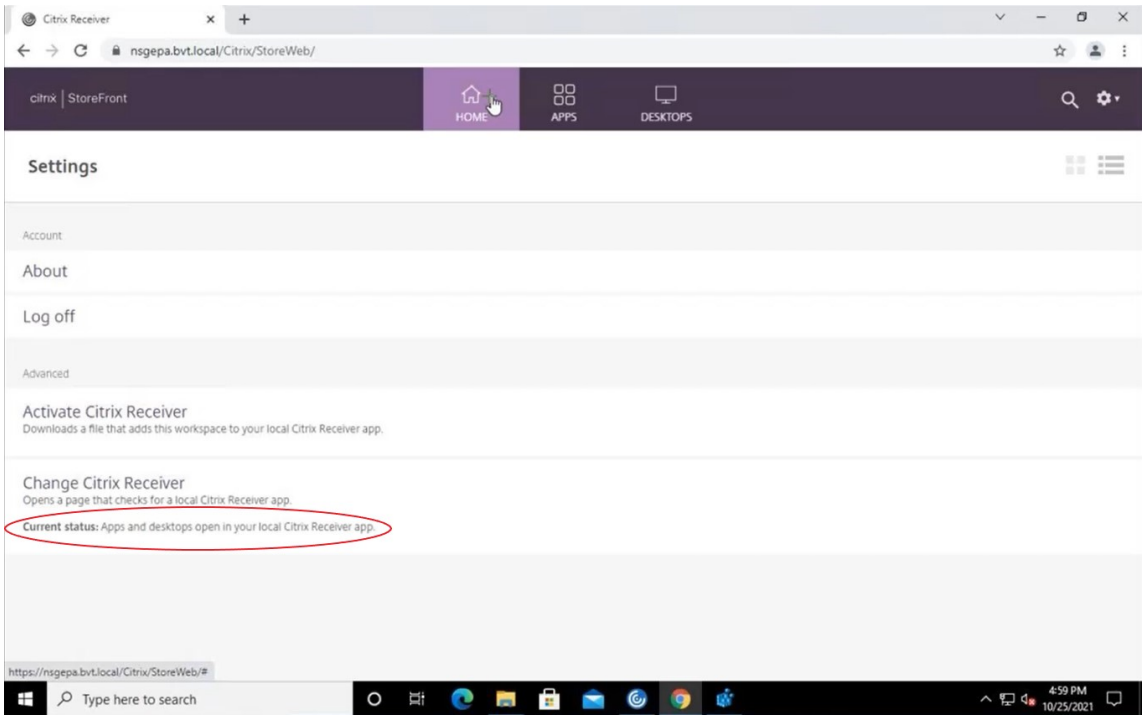
© 1999–2024 Cloud Software Group, Inc. All rights reserved.

4. Inicie de nuevo los servicios **IISADMIN** y **CitrixSubscriptionsStore** ejecutando los siguientes comandos:

```
sc start IISADMIN
sc start CitrixSubscriptionsStore
<!--NeedCopy-->
```

Experiencia de usuario final con el inicio híbrido para recursos protegidos

1. Tras la implementación de la solución por parte del administrador en el servidor de StoreFront, inicie sesión en el almacén en el lado del cliente y, a continuación, acceda a StoreFront mediante la URL en un explorador web.
2. Para comprobar si la aplicación Citrix Workspace se ha detectado correctamente en el explorador web, compruebe el **estado actual** en **Parámetros de cuenta**.



Una vez detectada la aplicación Citrix Workspace, puede ver e iniciar todas las aplicaciones y escritorios virtuales habilitados con App Protection.

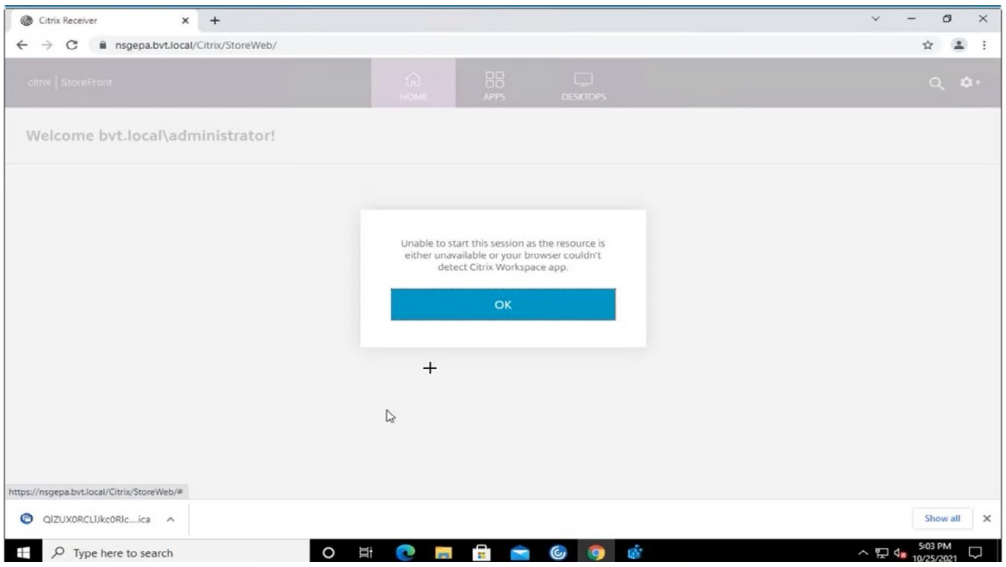
Habilitar el rastreo en StoreFront

Para habilitar el rastreo en StoreFront, consulte la documentación de StoreFront. Este rastreo se puede utilizar para verificar si las etiquetas configuradas de directiva de sesión de NetScaler Gateway se transmiten correctamente al almacén.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

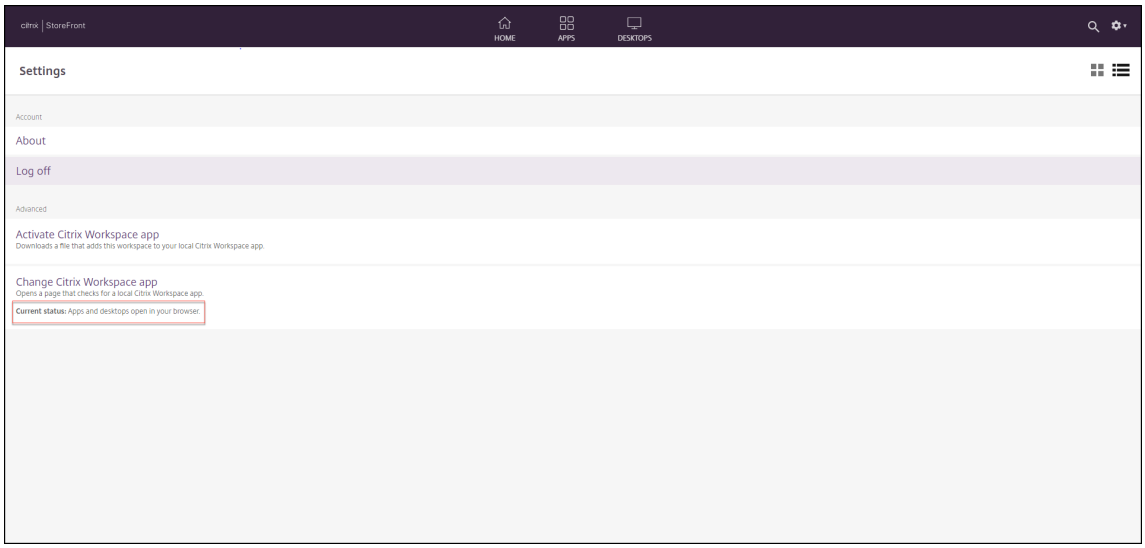
Solución de problemas

Al iniciar las sesiones habilitadas para App Protection, es posible que, a veces, se encuentre con este error:



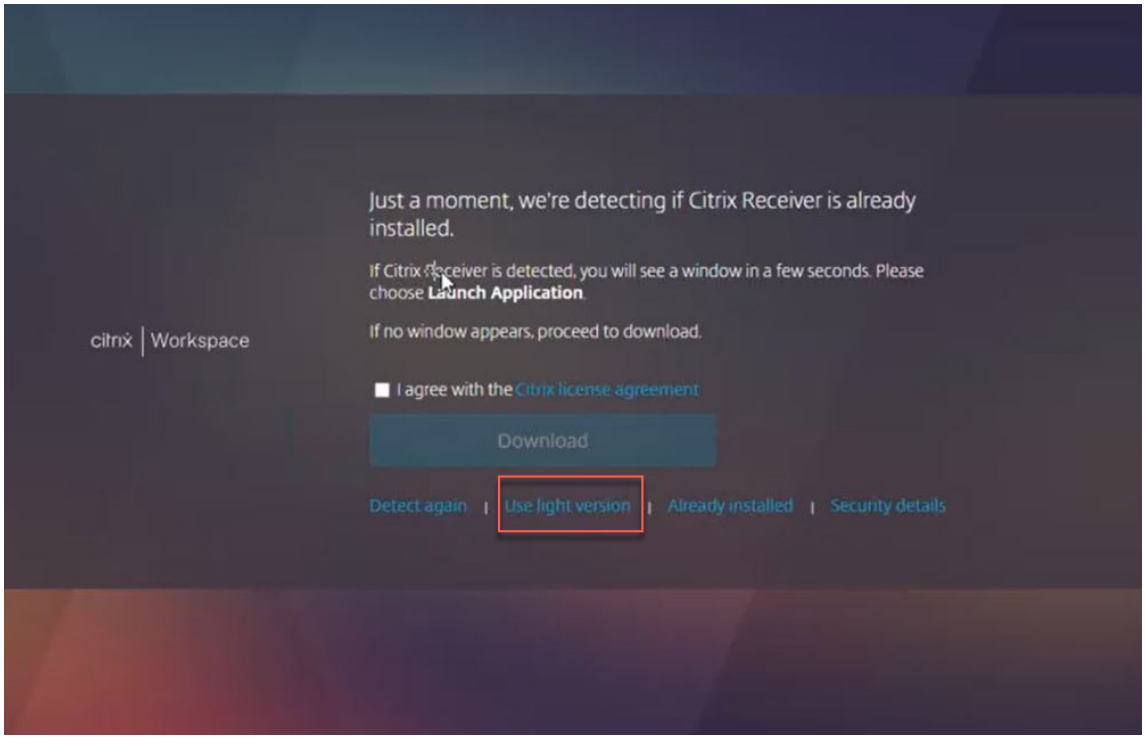
Los posibles motivos de este error son los siguientes:

- Las aplicaciones y los escritorios están configurados para abrirse en un explorador.

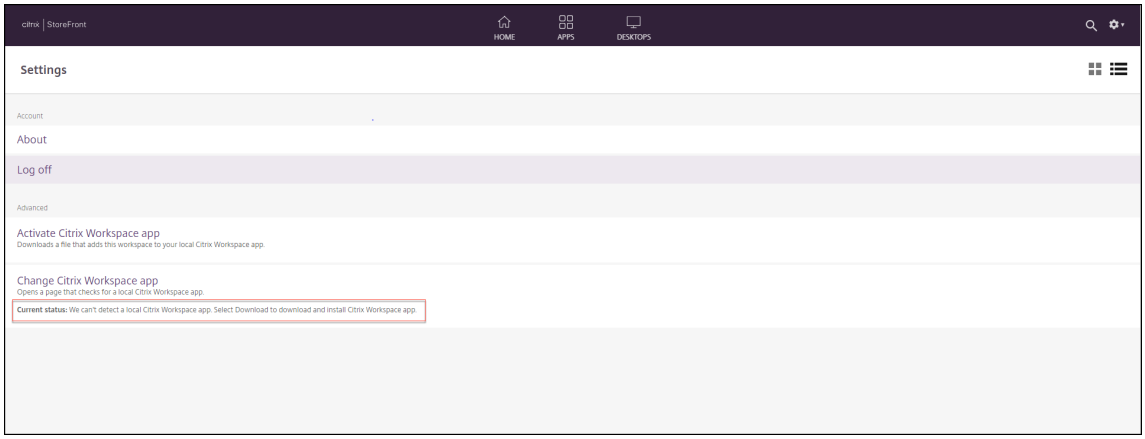


Se presenta esta situación si hizo clic en **Usar versión simplificada** durante la detección de la aplicación Citrix Workspace, como se muestra en la siguiente pantalla:

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

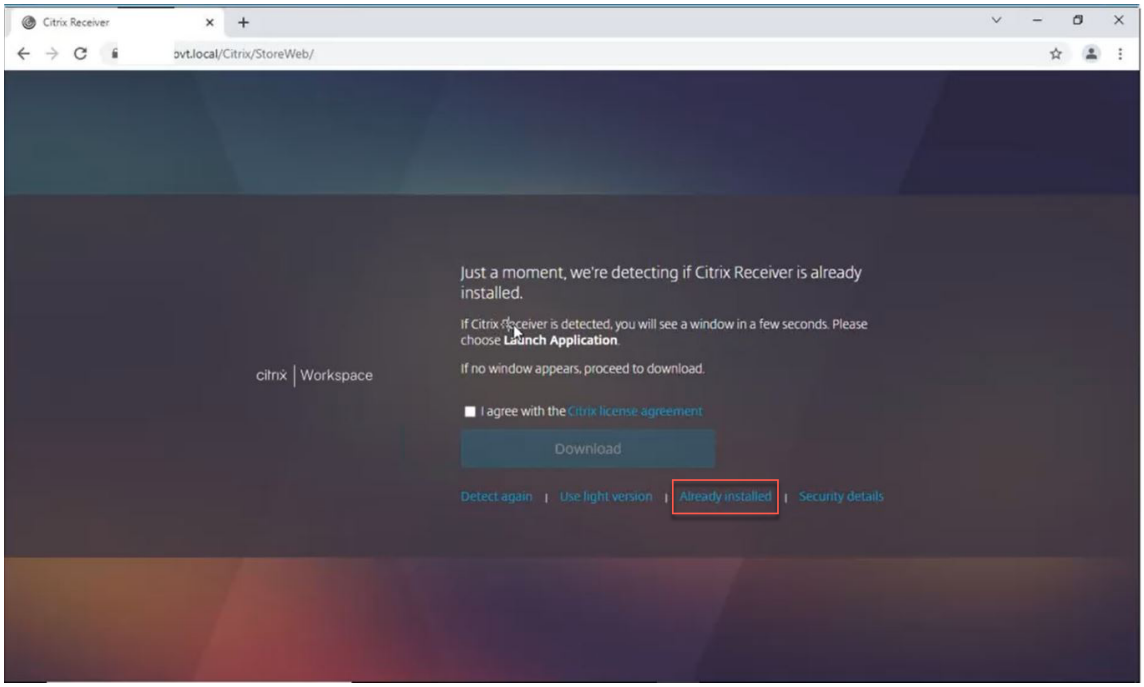


- El explorador web no detecta la aplicación Citrix Workspace.



Se presenta esta situación si hizo clic en **Ya instalado** durante la detección de la aplicación Citrix Workspace, como se muestra en la siguiente pantalla:

© 1999–2024 Cloud Software Group, Inc. All rights reserved.



Solución: para corregir los casos anteriores e iniciar las sesiones habilitadas para App Protection, haga clic en **Cambiar la aplicación Citrix Workspace** en **Parámetros de cuenta** y espere a que se detecte la aplicación Citrix Workspace.

Optimización

La detección de la aplicación Citrix Workspace es necesaria para poder iniciar las sesiones habilitadas para App Protection. Para evitar errores durante los inicios híbridos de sesiones protegidas, los administradores de StoreFront pueden utilizar la acción `ApplyUICustomization` del comando `deploy-solution.ps1` y ocultar las opciones **Usar versión simplificada** y **Ya instalado**.

Calendario de publicación de versiones de la aplicación Citrix Workspace

April 25, 2024

Este calendario de publicaciones ilustra la frecuencia y las fechas de publicación de las versiones de la aplicación Citrix Workspace. Aunque las fechas exactas pueden cambiar, queremos ayudarle a planificar con antelación. También queremos facilitarle la administración de las implementaciones de la aplicación Citrix Workspace.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

Las nuevas versiones pueden descargarse desde la página Descargas de la aplicación Citrix Workspace. La aplicación Citrix Workspace para Android, la aplicación Citrix Workspace para iOS y la aplicación Citrix Workspace para Windows (Tienda) también están disponibles para su descarga en sus respectivas tiendas de aplicaciones. Si ha habilitado Actualizaciones de Citrix Workspace para la aplicación Citrix Workspace para Mac o Windows, se le notificará para que acepte la descarga y la instalación de la actualización. Considere la posibilidad de suscribirse a nuestro feed RSS para recibir alertas cuando estén disponibles las nuevas versiones.

Para obtener información detallada sobre las funciones disponibles en cada aplicación Citrix Workspace, consulte Tabla de funciones de la aplicación Citrix Workspace.

Para obtener información sobre los ciclos de vida, consulte Lifecycle Milestones for Citrix Workspace app.

Frecuencia de publicación prevista

Las siguientes plataformas de la aplicación Citrix Workspace tienen una frecuencia de publicación trimestral:

- Linux
- Mac
- Windows

Las siguientes plataformas de la aplicación Citrix Workspace tienen una frecuencia de publicación de seis semanas:

- ChromeOS
- HTML5

Las siguientes plataformas de la aplicación Citrix Workspace tienen una frecuencia de publicación mensual:

- Android
- iOS

> **Nota:**
>
> La aplicación Citrix Workspace para Windows, la aplicación Citrix Workspace para Mac, la aplicación Citrix Workspace para Android y la aplicación Citrix Workspace para iOS de ahora en adelante tendrán versiones principales y secundarias dentro de un trimestre. Las versiones secundarias se denominarán ".10"e incluirán pequeñas mejoras de calidad y rendimiento. No se espera que la versión secundaria ".10"incluya nuevas funcionalidades importantes.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

Fechas de publicación previstas para las aplicaciones de escritorio

Aplicación Citrix Workspace	Febrero de 2024	Marzo de 2024	Abril de 2024	Mayo de 2024	Junio de 2024	Julio de 2024	Agosto de 2024	Septiembre de 2024	Octubre de 2024	Noviembre de 2024	Diciembre de 2024
Windows		-	☑	☑	☒	-	☑	☒	-	☑	-
Windows LTSR	☒	-	☑	-	☒	-	-	☒	-	-	☒
Mac	-	-	☑	☑	☒	-	☑	☒	-	☑	-
ChromeOS y HTML5	☒	-	☑	☑	☑	-	☑	☑	☑	-	☑
Linux	-	☑	-	☑	-	-	☑	-	-	☑	-

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

Aplicación Citrix Workspace	Febrero de 2024	Marzo de 2024	Abril de 2024	Mayo de 2024	Junio de 2024	Julio de 2024	Agosto de 2024	Septiembre de 2024	Octubre de 2024	Noviembre de 2024	Diciembre de 2024
Nota: El símbolo ☑ indica versiones principales y el símbolo ☒ indica versiones secundarias. El símbolo ☒ indica actualizaciones acumulativas (Cumulative Update, CU).											

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

Fechas de publicación previstas de aplicaciones para móviles y tabletas

La aplicación Citrix Workspace para Android y la aplicación Citrix Workspace para iOS tienen una frecuencia de publicación mensual.

Aplicación Citrix Workspace	Marzo de 2024	Abril de 2024	Mayo de 2024	Junio de 2024	Julio de 2024	Agosto de 2024	Septiembre de 2024	Octubre de 2024	Noviembre de 2024	Diciembre de 2024
Android e iOS	☑	☒	☑	☒	☑	☒	☑	☒	☑	☒

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

Aplicación Citrix Workspace	Marzo de 2024	Abril de 2024	Mayo de 2024	Junio de 2024	Julio de 2024	Agosto de 2024	Septiembre de 2024	Octubre de 2024	Noviembre de 2024	Diciembre de 2024
Nota: El símbolo ☑ indica versiones principales y el símbolo ☒ indica versiones secundarias. Las versiones secundarias son versiones opcionales adaptadas a necesidades o mejoras específi-										

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

> **Renuncia de responsabilidades:**
>
> El desarrollo, la publicación y el calendario descritos para nuestros productos permanece a nuestra propia discreción y están sujetos a cambios sin previo aviso ni consulta. Los datos suministrados tienen fines exclusivamente informativos y no suponen ningún compromiso, promesa ni obligación legal para entregar material, código ni funcionalidad, por lo que no deben utilizarse como factor para tomar decisiones de compra ni incorporarse en ningún contrato.

Tabla de funciones de la aplicación Citrix Workspace

April 25, 2024

La aplicación Citrix Workspace proporciona una gama de funciones distribuidas en diferentes plataformas o sistemas operativos. Con esta tabla de funciones, podrá comprender claramente la disponibilidad de las funciones en las diferentes plataformas. En cada sección, junto con la tabla de funciones, podrá ver la tabla de definición de funciones que describe brevemente cada función.

Citrix Workspace

Función	Windows 2311.1 y Tienda Windows 2309.1	Windows 2402 LTSR	Linux 2402	Mac 2402	iOS 24.3.5	Android 24.3.5	HTML5 2404	ChromeOS 2402.1
Citrix Virtual Apps	Sí	Sí	Sí	Sí	Sí	Sí	Sí	Sí
Citrix Virtual Desktops	Sí	Sí	Sí	Sí	Sí	Sí	Sí	Sí
Citrix Secure Private Access	Sí	Sí	No	Sí	Sí	Sí	No	No

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

Función	Windows 2311.1 y Tienda Windows 2309.1	Windows 2402 LTSR	Linux 2402	Mac 2402	iOS 24.3.5	Android 24.3.5	HTML5 2404	ChromeOS 2402.1
Citrix Enterprise Browser (anteriormente, Citrix Workspace Browser)	Sí	No	Sí	Sí	No	No	No	No
Aplicaciones web/SaaS con SSO	Sí	Sí	Sí	Sí	Sí	Sí	Sí	Sí
Aplicaciones móviles de Citrix	No	No	No	No	Sí	Sí	No	No
Servicio de personalización de aplicaciones	Sí	No	No	Sí	Sí	Sí	No	No

Función	Definición
Citrix Virtual Apps	Acceda a Citrix Virtual Apps a través del derecho de uso de Citrix DaaS o Citrix Virtual Apps and Desktops.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

Función	Definición
Citrix Virtual Desktops	Acceda a Citrix Virtual Desktops a través del derecho de uso de Citrix DaaS o Citrix Virtual Apps and Desktops.
Citrix Secure Private Access	Con Citrix Secure Private Access, los administradores de TI pueden controlar el acceso a las aplicaciones SaaS aprobadas. Además, con una experiencia de Single Sign-On simplificada, los administradores pueden filtrar el acceso a sitios web y categorías de sitios web específicos para proteger la red de la organización y los dispositivos de los usuarios finales contra malware y filtraciones de datos.
Citrix Enterprise Browser	El explorador web se entrega con la aplicación Citrix Workspace para acceder a aplicaciones SaaS y web de forma segura.
Aplicaciones web/SaaS con SSO	Acceda a aplicaciones web o SaaS configuradas mediante Secure Workspace Access con SSO.
Aplicaciones móviles de Citrix	Acceda a aplicaciones móviles de Citrix agregadas por Citrix Endpoint Management, antes conocidas como XenMobile.
Actualizaciones de versión de las aplicaciones móviles de Citrix	Acceda a aplicaciones móviles de Citrix agregadas por Citrix Endpoint Management, antes conocidas como XenMobile.
Servicio de personalización de aplicaciones	Permite tener una experiencia corporativa personalizada. Puede tener un nombre de aplicación personalizado y un icono de marca compartida para la aplicación Citrix Workspace en todo el flujo de trabajo de las aplicaciones.

Administración de Workspace

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

Función	Windows 2311.1 y Tienda Windows 2309.1	Windows 2402 LTSR	Linux 2402	Mac 2402	iOS 24.3.5	Android 24.3.5	HTML5 2404	ChromeOS 2402.1
Configuración automática mediante DNS para la detección de correo electrónico	Sí	Sí	No	Sí	Sí	Sí	No	No
Parámetros de administración centralizada	Sí	Sí	Sí	No	No	No	No	Sí
Global App Config Service (Workspace)	Sí	Sí	No	Sí	Sí	Sí	Sí	Sí
Global App Config Service (StoreFront)	Sí	Sí	No	Sí	Sí	Sí	Sí	Sí

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

Función	Windows 2311.1 y Tienda Windows 2309.1	Windows 2402 LTSR	Linux 2402	Mac 2402	iOS 24.3.5	Android 24.3.5	HTML5 2404	ChromeOS 2402.1
Actualizaciones de la App Store	No	No	No	No	Sí	Sí	No	No
Actualizaciones automáticas de Citrix	Sí	Sí	No	Sí	No	No	No	No
Administración de aplicaciones cliente	Sí	No	No	No	No aplicable	No aplicable	No aplicable	No aplicable

Función	Definición
Configuración automática mediante DNS para la detección de correo electrónico	Permite que la aplicación Citrix Workspace se pueda configurar con parámetros de detección automática.
Parámetros de administración centralizada	Parámetro de aplicaciones desde un servicio centralizado. Por ejemplo: administración de Google Chrome o GPO.
Global App Config Service (Workspace)	Citrix Global App Configuration Service para Citrix Workspace ofrece a los administradores de Citrix la capacidad de entregar direcciones URL de servicio de Workspace y parámetros de la aplicación Citrix Workspace a través de un servicio administrado de forma centralizada.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

Función	Definición
Global App Config Service (StoreFront)	Global App Configuration Service para Citrix StoreFront permite a los administradores de Citrix entregar parámetros de la aplicación Citrix Workspace a través de un servicio administrado de forma centralizada.
Actualizaciones de la App Store	Actualizaciones de la tienda de aplicaciones del proveedor
Actualizaciones automáticas de Citrix	Actualizaciones para Windows y Mac a través de la función de actualización automática de Citrix
Administración de aplicaciones cliente	Permite que la aplicación Citrix Workspace se convierta en una aplicación cliente única que se necesita en el dispositivo de punto final para instalar y administrar agentes, como el agente de Secure Access y el plug-in de End Point Analysis (EPA). Con esta función, los administradores pueden implementar y administrar fácilmente los agentes necesarios desde una única consola de administración.

Interfaz de usuario

Función	Windows 2311.1 y Tienda Windows 2309.1	Windows 2402 LTSR	Linux 2402	Mac 2402	iOS 24.3.5	Android 24.3.5	HTML5 2404	ChromeOS 2402.1
Desktop Viewer / Barra de escritorio	Sí	Sí	Sí	Sí	Sí	Sí	Sí	Sí
Entorno multitarea	Sí	Sí	Sí	Sí	Sí	Sí	Sí	Sí

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

Función	Windows 2311.1 y Tienda Windows 2309.1	Windows 2402 LTSR	Linux 2402	Mac 2402	iOS 24.3.5	Android 24.3.5	HTML5 2404	ChromeOS 2402.1
Sesiones de seguimiento (control del espacio de trabajo)	Sí	Sí	Sí	Sí	Sí	Sí	Sí	Sí

Función	Definición
Desktop Viewer / Barra de escritorio	Permite el control de funciones de la sesión, como enviar el comando Ctrl+Alt+Supr a través de una barra de herramientas.
Entorno multitarea	Permite usar varias aplicaciones y escritorios al mismo tiempo.
Sesiones de seguimiento (control del espacio de trabajo)	Permite a los usuarios pasar de un dispositivo a otro y conectarse automáticamente a todas sus sesiones.

Núcleo de host HDX

Función	Windows 2311.1 y Tienda Windows 2309.1	Windows 2402 LTSR	Linux 2402	Mac 2402	iOS 24.3.5	Android 24.3.5	HTML5 2404	ChromeOS 2402.1
Transporte adaptable	Sí	Sí	Sí	Sí	Sí	Sí	No	No

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

Función	Windows 2311.1 y Tienda Windows 2309.1	Windows 2402 LTSR	Linux 2402	Mac 2402	iOS 24.3.5	Android 24.3.5	HTML5 2404	ChromeOS 2402.1
Rendimiento HDX adaptable	Sí	Sí	No	No	No	No	No	No
Compatibilidad con SDWAN	Sí	Sí	Sí	Sí	No	No	Sí	Sí
Fiabilidad de la sesión	Sí	Sí	Sí	Sí	Sí	Sí	Sí	Sí
Reconexión automática de clientes	Sí	Sí	Sí	Sí	No	Sí	No	No
Sesiones compartidas	Sí	Sí	Sí	Sí	Sí	Sí	Sí	Sí
ICA multipuerto	Sí	Sí	Sí	No	No	No	No	No

Función	Definición
Transporte adaptable	Permite el transporte EDT para HDX para mejorar el rendimiento independientemente de las condiciones de la red.
Compatibilidad con SDWAN	Permite la aceleración de SDWAN para QoS, TCP, compresión y desduplicación.
Fiabilidad de la sesión	Mantiene las sesiones activas y en la pantalla del usuario cuando la conectividad de red se ve interrumpida.
Reconexión automática de clientes	Solicita y conectar de nuevo la sesión en caso de interrupción de la conexión.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

Función	Definición
Sesiones compartidas	Permite que la aplicación publicada se ejecute en la misma conexión que otras aplicaciones publicadas cuando ya se está ejecutando en el mismo servidor.
ICA multipuerto	Permite el uso de varios puertos TCP para el tráfico HDX con el fin de mejorar la calidad del servicio.

E/S de HDX / Dispositivos / Impresión

Función	Windows 2311.1 y Tienda Windows 2309.1	Windows 2402 LTSR	Linux 2402	Mac 2402	iOS 24.3.5	Android 24.3.5	HTML5 2404	ChromeOS 2402.1
Impresión local	Sí	Sí	Sí	Sí	Sí	No	Sí	Sí
Redirección de USB genérico	Sí	Sí	Sí	Sí	Sí	Sí	Sí	Sí
Asignación de unidades del cliente / Transferencia de archivos	Sí	Sí	Sí	Sí	Sí	Sí	Sí	Sí
TWAIN 2.0	Sí	No	No	No	No	No	No	No

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

Función	Definición
Impresión local	Permite a los usuarios imprimir documentos a través de impresoras compartidas o locales.
Redirección de USB genérico	Permite el uso de dispositivos USB dentro de las sesiones. Por ejemplo, teclado, ratón, cámara web externa, etc.
Asignación de unidades del cliente / Transferencia de archivos	Permite el uso de unidades del cliente integradas o conectadas para el almacenamiento de datos.
TWAIN	Permite la asignación de dispositivos cliente TWAIN, como cámaras digitales o escáneres.

Integración de HDX

Función	Windows 2311.1 y Tienda Windows 2309.1	Windows 2402 LTSR	Linux 2402	Mac 2402	iOS 24.3.5	Android 24.3.5	HTML5 2404	ChromeOS 2402.1
Acceso a aplicaciones locales	Sí	Sí	No	No	No	No	No	No
Multitoque	Sí	Sí	No	No	Sí	Sí	Sí	Sí
Mobility Pack	Sí	Sí	No	No	Sí	Sí	Sí	Sí
HDX Insight	Sí	Sí	Sí	Sí	No	No	Sí	Sí
HDX Insight con el canal virtual de NSAP	Sí	Sí	Sí	Sí	Sí *(3)*	Sí *(3)*	No	No

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

Función	Windows 2311.1 y Tienda Windows 2309.1	Windows 2402 LTSR	Linux 2402	Mac 2402	iOS 24.3.5	Android 24.3.5	HTML5 2404	ChromeOS 2402.1
Tabla de experiencia de supervisión EUEM	Sí	Sí	Sí	Sí	No	Sí	Sí	Sí
Redirección bidireccional de contenido	Sí	Sí	No	No	No	No	No	No
Redirección de URL	Sí	Sí	Sí	Sí	Sí	Sí	Sí	Sí
Redirección de contenido del explorador web	Sí	No	Sí	No	No	No	No	Sí
Abrir archivos en la aplicación Citrix Workspace	Sí	Sí	Sí	No	Sí	Sí	No	Sí

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

Función	Windows 2311.1 y Tienda Windows 2309.1	Windows 2402 LTSR	Linux 2402	Mac 2402	iOS 24.3.5	Android 24.3.5	HTML5 2404	ChromeOS 2402.1
Servicios basados en la ubicación (ubicación disponible a través de la descripción de la API)	Sí	Sí	No	No	Sí	Sí	No	No

Función	Definición
Acceso a aplicaciones locales	Acceda a aplicaciones locales en dispositivos cliente dentro de las sesiones.
Multitoque	Permite el control multitáctil con 10 dedos de escritorios y aplicaciones Windows/Linux.
Mobility Pack	Habilita funciones de experiencia nativa del dispositivo (por ejemplo, teclado emergente automático y controles de interfaz de usuario del dispositivo local) y escritorios optimizados para tabletas.
HDX Insight	Proporciona visibilidad sobre las horas de inicio y finalización de las sesiones mediante métricas de rendimiento de la red ICA.
HDX Insight con el canal virtual de NSAP	Proporciona visibilidad sobre la hora de inicio y finalización de las sesiones mediante NetScaler App Experience o el canal virtual de NSAP para obtener información sobre HDX.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

Función	Definición
Tabla de experiencia de supervisión EUEM	Proporciona a los administradores de Citrix visibilidad sobre las métricas de duración de los inicios de sesión a través del Citrix Virtual Desktop, antes denominado XenDesktop 7 Director.
Redirección bidireccional de contenido	Permite la redirección de URL del cliente al host y del host al cliente.
Redirección de URL	Permite ejecutar aplicaciones de forma local en el cliente.
Redirección de contenido del explorador web	Permite redirigir una página web completa (la ventanilla de un explorador web) al dispositivo de punto final para la representación local, lo que libera al servidor de carga.
Abrir archivos en la aplicación Citrix Workspace	Permite abrir un archivo local en la aplicación Citrix Workspace mediante una aplicación alojada (redirección de contenido del cliente al servidor).
Servicios basados en la ubicación (ubicación disponible a través de la descripción de la API)	Permite que la información de ubicación sea utilizada por aplicaciones entregadas por Citrix Virtual Desktop, antes denominado XenDesktop.

HDX multimedia

Función	Windows 2311.1 y Tienda Windows 2309.1	Windows 2402 LTSR	Linux 2402	Mac 2402	iOS 24.3.5	Android 24.3.5	HTML5 2404	ChromeOS 2402.1
Reproducción de audio	Sí	Sí	Sí	Sí	Sí	Sí	Sí	Sí
Audio bidireccional (VoIP)	Sí	Sí	Sí	Sí	Sí	Sí	Sí	Sí

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

Función	Windows 2311.1 y Tienda Windows 2309.1	Windows 2402 LTSR	Linux 2402	Mac 2402	iOS 24.3.5	Android 24.3.5	HTML5 2404	ChromeOS 2402.1
Redirección de cámaras web	Sí	Sí	Sí	Sí	Sí	Sí	Sí	Sí
Reproducción de vídeo	Sí	Sí	Sí	Sí	Sí	Sí	Sí	Sí
Optimización de Microsoft Teams	Sí	Sí	Sí (solo x64)	Sí	No	No	Sí	Sí
Optimization Pack para Skype Empresarial	Sí	Sí	Sí	Sí	No	No	No	No
Optimización de comunicaciones unificadas de Cisco Jabber	Sí	Sí	Sí	No	No	No	No	No
Redirección multimedia de Windows	Sí	Sí	Sí	No	No	No	No	No
Audio UDP	Sí	Sí	Sí	No	No	No	No	No

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

Función	Definición
Reproducción de audio	Permite la reproducción de audio generado en el servidor.
Audio bidireccional (VoIP)	Permite el uso de aplicaciones de colaboración alojadas de softphone/chat de voz.
Redirección de cámaras web	Permite el uso de aplicaciones de colaboración de chat de vídeo mediante una cámara web local.
Reproducción de vídeo	Permite la visualización de vídeos grabados.
Optimización de Microsoft Teams	Descarga el procesamiento multimedia de Microsoft Teams del servidor de Citrix al dispositivo del usuario.
Optimización de Skype Empresarial	Descarga el procesamiento multimedia de Skype Empresarial del servidor de Citrix al dispositivo del usuario. En el caso de la aplicación Citrix Workspace para Android, solo está disponible en dispositivos Chrome.
Optimización de comunicaciones unificadas de Cisco Jabber	Descarga el procesamiento multimedia de Jabber del servidor de Citrix al dispositivo del usuario.
Redirección multimedia de Windows	Permite representar archivos multimedia de Windows en el dispositivo del usuario, al tiempo que libera la carga del servidor.
Audio UDP	Compatibilidad con la entrada y la salida de audio a través de UDP.

Seguridad

Función	Windows 2311.1 y Tienda Windows 2309.1	Windows 2402 LTSR	Linux 2402	Mac 2402	iOS 24.3.5	Android 24.3.5	HTML5 2404	ChromeOS 2402.1
TLS 1.2	Sí	Sí	Sí	Sí	Sí	Sí	Sí	Sí

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

Función	Windows 2311.1 y Tienda Windows 2309.1	Windows 2402 LTSR	Linux 2402	Mac 2402	iOS 24.3.5	Android 24.3.5	HTML5 2404	ChromeOS 2402.1
TLS 1.0/1.1	Sí	Sí	Sí	Sí	Sí	Sí	Sí	Sí
DTLS 1.0	Sí	Sí	Sí	Sí	Sí	Sí	No	No
DTLS 1.2	Sí	Sí	Sí	Sí	No	No	No	No
Certificado SHA2	Sí	Sí	Sí	Sí	Sí	Sí	Sí	Sí
Acceso inteligente	Sí	Sí	Sí	Sí	Sí	Sí	Sí	Sí
Acceso remoto a través de Citrix Gateway	Sí *(1)*	Sí	Sí	Sí	Sí	Sí	Sí	Sí
Acceso a Workspace para Web	Sí	Sí	Sí	Sí	A través de un archivo ICA	Sí	Sí	Sí
IPV6	Sí	Sí	Sí	Sí	Sí	Sí	Sí	Sí
App Protection	Sí	Sí	Sí	Sí	No	No	No	No

Función	Definición
TLS 1.2	Sucesor de SSL, seguridad reforzada en canales de comunicación.
TLS 1.0/1.1	Sucesor de SSL, seguridad reforzada en canales de comunicación.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

Función	Definición
DTLS 1.0	DTLS es una derivación del protocolo SSL. Proporciona los mismos servicios de seguridad (integridad, autenticación y confidencialidad), pero bajo el protocolo UDP.
DTLS 1.2	DTLS es una derivación del protocolo SSL. Proporciona los mismos servicios de seguridad (integridad, autenticación y confidencialidad), pero bajo el protocolo UDP.
Certificado SHA2	Capacidad para usar certificados SHA2.
Acceso inteligente	Controla el acceso a aplicaciones disponibles mediante directivas y filtros de Gateway.
Acceso remoto a través de Gateway	Proporciona a los usuarios acceso seguro a aplicaciones empresariales, escritorios virtuales y datos en cualquier lugar sin el cliente de ninguna VPN.
Acceso a Workspace para Web	Acceso a aplicaciones alojadas o escritorios virtuales mediante un explorador web.
IPV6	Permite su uso en redes IPV6.

Gráficos HDX

Función	Windows 2311.1 y Tienda Windows 2309.1	Windows 2402 LTSR	Linux 2402	Mac 2402	iOS 24.3.5	Android 24.3.5	HTML5 2404	ChromeOS 2402.1
SuperCodec mejorado con H.264	Sí	Sí	Sí	Sí	Sí	Sí	Sí	Sí
Aceleración de hardware del cliente	Sí	Sí	Sí	Sí	No	Sí	No	No

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

Función	Windows 2311.1 y Tienda Windows 2309.1	Windows 2402 LTSR	Linux 2402	Mac 2402	iOS 24.3.5	Android 24.3.5	HTML5 2404	ChromeOS 2402.1
Gráficos 3DPro	Sí	Sí	Sí	Sí	Sí	Sí	Sí	Sí
Compatibilidad con monitores externos	Sí	Sí	Sí	Sí	Sí	Sí	Sí	Sí
Redirección de composición del escritorio	Sí	Sí	No	No	No	No	No	No
Entorno multimonitor real	Sí	Sí	Sí	Sí	No	No	Sí	Sí

Función	Definición
SuperCodec mejorado con H.264	Permite la entrega optimizada de aplicaciones mediante SuperCodec mejorado con H264 de XenApp/Desktop 7.X.
Aceleración de hardware del cliente	Permite la aceleración de hardware para funciones HDX como gráficos y cámara web. El uso de la capacidad de hardware varía según las diferentes aplicaciones de Citrix Workspace.
Gráficos 3DPro	Permite el uso de aplicaciones profesionales de gráficos 3D alojadas en el centro de datos.
Compatibilidad con monitores externos	Permite el uso de un monitor externo.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

Función	Definición
Redirección de composición del escritorio	Habilita el comando de gráficos que es remoto para el cliente para la representación gráfica y, así, garantizar la escalabilidad del servidor. Elemento retirado en la versión 12.9 de Receiver para Mac.
Entorno multimonitor real	XenApp o XenDesktop crean la misma cantidad de monitores que admite el cliente.

Autenticación

Función	Windows 2311.1 y Tienda Windows 2309.1	Windows 2402 LTSR	Linux 2402	Mac 2402	iOS 24.3.5	Android 24.3.5	HTML5 2404	ChromeOS 2402.1
Autenticación federada (SAML/Azure AD)	Sí	Sí	Sí	Sí	Sí	Sí	Sí	Sí
VPN completa de ADC	Sí	Sí	Sí	Sí	No	No	No	No
Token de software de RSA	No	No	No	No	Sí	Sí	No	No

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

Función	Windows 2311.1 y Tienda Windows 2309.1	Windows 2402 LTSR	Linux 2402	Mac 2402	iOS 24.3.5	Android 24.3.5	HTML5 2404	ChromeOS 2402.1
SMS de respuesta a desafíos (RADIUS)	Sí	Sí	No	Sí	No	No	No	No
Autenticación de certificados de usuario mediante Gateway (mediante la aplicación nativa de Workspace)	No	No	No	No	Sí	Sí	Sí	Sí

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

Función	Windows 2311.1 y Tienda Windows 2309.1	Windows 2402 LTSR	Linux 2402	Mac 2402	iOS 24.3.5	Android 24.3.5	HTML5 2404	ChromeOS 2402.1
Autenticación de certificados de usuario a través de Gateway (mediante explorador web)	Sí *(4)*	Sí *(4)*	No	Sí	No	No	Sí	Sí
Tarjeta inteligente (CAC, PIV, etc.)	Sí	Sí	Sí	Sí	Sí	Sí	No	Sí
Tarjeta de proximidad/sin contacto	Sí	Sí	Sí	No	No	No	No	Sí

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

Función	Windows 2311.1 y Tienda Windows 2309.1	Windows 2402 LTSR	Linux 2402	Mac 2402	iOS 24.3.5	Android 24.3.5	HTML5 2404	ChromeOS 2402.1
Inserción de credenciales (por ejemplo, Fast Connect, Storebrowse)	Sí	Sí	Sí	No	No	No	No	Sí
Autenticación PassThrough	Sí	Sí	No	No	No	No	No	No
Guardar credenciales *Localmente y solo en StoreFront	Sí	Sí	No	Sí	No	No	No	No
Autenticación nFactor de ADC	Sí	Sí	Sí	Sí	Sí	Sí	Sí	Sí
Contraseña de un solo uso nativa de ADC	Sí	Sí	Sí	Sí	Sí	Sí	Sí	Sí

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

Función	Windows 2311.1 y Tienda Windows 2309.1	Windows 2402 LTSR	Linux 2402	Mac 2402	iOS 24.3.5	Android 24.3.5	HTML5 2404	ChromeOS 2402.1
Autenticación biométrica (Touch ID, Face ID)	No	No	No	No	Sí	No	No	No
Single Sign-On en aplicaciones móviles de Citrix	No	No	No	No	Sí	Sí	No	No
Acceso anónimo a almacenes	Sí	Sí	Sí	Sí	Sí	Sí	Sí	Sí

Función	Definición
Autenticación federada (SAML/Azure AD)	Habilita el servidor de FAS para la autenticación de usuarios que delega el servidor de Microsoft ADFS (u otro IdP compatible con SAML) mediante Azure AD o SAML.
VPN completa de ADC (NetScaler)	Crea un túnel VPN completo para Gateway.
Token de software de RSA	Permite la autenticación simplificada al usar tokens de software de RSA.
SMS de respuesta a desafíos (RADIUS)	Permite el uso de la autenticación de respuesta a desafíos. Por ejemplo: el uso de códigos de acceso por SMS.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

Función	Definición
Autenticación de certificados de usuario mediante Gateway (solo a través del explorador web)	Permite el uso de certificados de usuario como un factor de autenticación con Gateway, que es para la autenticación por explorador web en Windows.
Tarjeta inteligente (CAC, PIV, etc.)	Permite el uso de una tarjeta inteligente criptográfica compatible con PC/SC estándar para la autenticación y la firma.
Tarjeta de proximidad/sin contacto	Permite a los usuarios usar aplicaciones o escritorios de Citrix mediante la autenticación con tarjetas inteligentes de proximidad o sin contacto.
Inserción de credenciales (por ejemplo, Fast Connect, Storebrowse)	Permite a los usuarios usar aplicaciones o escritorios de Citrix mediante la autenticación con una tarjeta inteligente de proximidad o sin contacto. Storebrowse es una herramienta de utilidad con línea de comandos disponible con la aplicación Citrix Workspace para Windows. Puede usar Storebrowse para personalizar la aplicación Citrix Workspace mediante la creación de scripts de la utilidad Storebrowse.
Autenticación PassThrough	Transmite las credenciales de usuario a un sitio de interfaz web y, a continuación, a los servidores de Citrix Virtual Apps and Desktops. Este proceso impide que los usuarios se autentiquen de forma explícita en cualquier momento durante el proceso de inicio de las aplicaciones de Citrix.
Guardar credenciales *Localmente y solo en StoreFront	Permite guardar credenciales de manera local y solo mediante Citrix StoreFront.
Contraseña de un solo uso nativa de Gateway	Gateway admite contraseñas de un solo uso (OTP) sin tener que usar un servidor de terceros, ya que mantiene toda la configuración en el dispositivo NetScaler.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

Función	Definición
Autenticación nFactor de NetScaler	La autenticación nFactor permite flujos de autenticación dinámicos basados en el perfil del usuario. A veces, estos flujos pueden ser flujos simples para que resulten intuitivos al usuario. La versión mínima de NetScaler necesaria es 12.1.49.x.
Autenticación biométrica (Touch ID, Face ID)	Permite autenticaciones biométricas, como Touch ID y Face ID.
Single Sign-On en aplicaciones móviles de Citrix	Permite Single Sign-On en aplicaciones móviles de Citrix.
Acceso anónimo a almacenes	Acceso posible para usuarios no autenticados (anónimos).

Experiencia de las entradas de texto

Función	Windows 2311.1 y Tienda Windows 2309.1	Windows 2402 LTSR	Linux 2402	Mac 2402	iOS 24.3.5	Android 24.3.5	HTML5 2404	ChromeOS 2402.1
Sincronización de la distribución del teclado: Del cliente al VDA (Windows VDA)	Sí	Sí	Sí	Sí	Sí	Sí	No	No

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

Función	Windows 2311.1 y Tienda Windows 2309.1	Windows 2402 LTSR	Linux 2402	Mac 2402	iOS 24.3.5	Android 24.3.5	HTML5 2404	ChromeOS 2402.1
Sincronización de la distribución del teclado: Del cliente al VDA (Linux VDA)	Sí	Sí	Sí	Sí	Sí	Sí	No	No
Sincronización de la distribución del teclado: Del VDA al cliente (Windows VDA)	No	No	No	No	No	No	No	No
Sincronización de la distribución del teclado: Del VDA al cliente (Linux VDA)	No	No	No	No	No	No	No	No

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

Función	Windows 2311.1 y Tienda Windows 2309.1	Windows 2402 LTSR	Linux 2402	Mac 2402	iOS 24.3.5	Android 24.3.5	HTML5 2404	ChromeOS 2402.1
Asignación de distribución de teclado Unicode	No	No	Sí	Sí	Sí	Sí	Sí	Sí
Modo de entrada de teclado: Unicode	No	No	Sí	Sí	Sí	Sí	Sí	Sí
Modo de entrada de teclado: Scancode	Sí	Sí	Sí	Sí	No	No	Sí	Sí
IME del servidor	Sí	Sí	Sí	Sí	Sí	Sí	Sí	Sí
IME de cliente genérico (CTXIME) para IME con CJK	Sí	Sí	No	Sí	Sí	Sí	Sí	Sí
Interfaz de línea de comandos	Sí	Sí	No	No	No	No	No	No

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

Función	Windows 2311.1 y Tienda Windows 2309.1	Windows 2402 LTSR	Linux 2402	Mac 2402	iOS 24.3.5	Android 24.3.5	HTML5 2404	ChromeOS 2402.1
Configuraciones interfaz de usuario de la sincronización del teclado	Sí	Sí	Sí	Sí	Sí	Sí	No	No
Configuraciones interfaz de usuario del modo de entrada	No	No	Sí	Sí	Sí	No	No	No
Configuraciones interfaz de usuario de la barra de idioma	Sí	Sí	No	Sí	No	No	No	No

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

Función	Definición
Sincronización de la distribución del teclado: Del cliente al VDA (Windows VDA)	Permite a los usuarios sincronizar las distribuciones del teclado activas o cambiar entre distribuciones preferidas en el dispositivo cliente. La distribución del teclado del dispositivo cliente se establece automáticamente en Windows VDA.
Sincronización de la distribución del teclado: Del cliente al VDA (Linux VDA)	Permite a los usuarios sincronizar las distribuciones del teclado activas o cambiar entre distribuciones preferidas en el dispositivo cliente. La distribución del teclado del dispositivo cliente se establece automáticamente en Linux VDA.
Sincronización de la distribución del teclado: Del VDA al cliente (Windows VDA)	Permite a los usuarios sincronizar las distribuciones de teclado activas o cambiar entre distribuciones preferidas en Windows VDA. La distribución del teclado de Windows VDA se establece automáticamente en el dispositivo cliente.
Sincronización de la distribución del teclado: Del VDA al cliente (Linux VDA)	Permite a los usuarios sincronizar las distribuciones de teclado activas o cambiar entre distribuciones preferidas en Linux VDA. La distribución del teclado en Linux VDA se establece automáticamente en el dispositivo cliente.
Asignación de distribución de teclado Unicode	Admite la asignación de la distribución de teclado Unicode para Windows VDA con una aplicación Citrix Workspace que no sea de Windows.
Modo de entrada de teclado: Unicode	El modo de entrada de Unicode envía la tecla del teclado del lado del cliente al VDA, y el VDA genera el mismo carácter en el VDA. Aplica la distribución del teclado del lado del cliente.
Modo de entrada de teclado: Scancode	El modo de entrada de Scancode envía la posición de la tecla del teclado del lado del cliente al VDA, y el VDA genera el carácter correspondiente. Aplica la distribución del teclado del lado del servidor.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

Función	Definición
IME del servidor	Proporciona usabilidad y experiencia con el editor de métodos de entrada (IME) del lado del servicio (o VDA).
IME de cliente genérico (CTXIME) para IME con CJK	Proporciona una mejor usabilidad del IME del cliente y una experiencia mejorada y fluida para los idiomas de Asia oriental (chino, japonés y coreano).
Interfaz de línea de comandos	Los usuarios pueden habilitar o inhabilitar el IME del cliente mediante las interfaces de línea de comandos.
Configuraciones e interfaz de usuario de la sincronización del teclado	Los usuarios pueden elegir diferentes opciones de sincronización de la distribución del teclado mediante la GUI.
Configuraciones e interfaz de usuario del modo de entrada	Los usuarios pueden elegir diferentes opciones de modo de entrada de teclado mediante la interfaz gráfica de usuario.
Configuraciones e interfaz de usuario de la barra de idioma	Los usuarios pueden optar por mostrar u ocultar la barra de idioma remota en una sesión de aplicación del VDA mediante la GUI. La barra de idioma muestra el idioma de entrada preferido en una sesión.
Plantilla administrativa de GPO para la sincronización de la distribución del teclado	Los administradores pueden supeditar las configuraciones de sincronización de la distribución del teclado mediante la implementación de las directivas correspondientes desde la plantilla administrativa de objetos de directiva de grupo de la aplicación Citrix Workspace.

Indicadores de la tabla

Indicador	Descripción
1	Solo StoreFront

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

Indicador	Descripción
2	HDX 3D Pro se revierte a JPEG para estas aplicaciones Citrix Workspace. Se recomiendan 3 Mbps frente a 1,5 Mbps con compresión profunda de H.264.
3	Para el canal virtual de NSAP, la aplicación Workspace para iOS/Android es compatible, pero, para ADC/ADM, todavía se está trabajando en ello.
4	La autenticación de certificados de usuario mediante Gateway (solo mediante explorador) no es compatible con la detección de clientes de la aplicación Citrix Workspace. Puede abrir una aplicación o un escritorio virtual con la aplicación Citrix Workspace solo si se descarga el archivo ICA.

Nota:

El desarrollo, la publicación y el calendario de funciones descritos para nuestros productos permanece a nuestra propia discreción. La información que se proporciona aquí tiene fines exclusivamente informativos y no supone un compromiso, una promesa ni una obligación legal para entregar material, código ni funcionalidad, por lo que no debe utilizarse como factor para tomar decisiones de compra ni incorporarse en ningún contrato. El desarrollo, la publicación y el calendario de funciones descritos para nuestros productos permanece a nuestra propia discreción y están sujetos a cambios sin previo aviso ni consulta.

© 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).