Aplicación Citrix Workspace para ChromeOS

Contents

Aplicación Citrix Workspace para ChromeOS

June 18, 2024

La aplicación Citrix Workspace para ChromeOS es una aplicación nativa empaquetada de Chrome que le permite acceder a aplicaciones y escritorios virtuales de Workspace alojados en Citrix desde dispositivos Chrome. Está disponible en Chrome Web Store.

Para obtener información detallada sobre funciones, problemas resueltos y problemas conocidos, consulte la página Acerca de esta versión.

Con la aplicación Citrix Workspace para ChromeOS instalada, puede acceder a escritorios y aplicaciones dentro de los exploradores web. No se necesitan opciones adicionales de configuración o implementación en StoreFront.

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

Para obtener información sobre los elementos retirados, consulte la página Elementos retirados.

Idiomas disponibles

La aplicación Citrix Workspace para ChromeOS está adaptada para usarse en otros idiomas que no son el inglés. Para obtener una lista de los idiomas disponibles en la aplicación Citrix Workspace para ChromeOS, consulte Idiomas disponibles.

Compatibilidad con ChromeOS LTS

Google tiene la versión de asistencia a largo plazo (LTS) en ChromeOS si prefiere menos actualizaciones. En cualquier momento, una o más versiones de la aplicación Citrix Workspace son compatibles con la versión más reciente de ChromeOS LTS.

Si busca una versión de la aplicación Citrix Workspace con las correcciones de errores y funciones más recientes, le recomendamos:

- Usar la versión más reciente de la aplicación Citrix Workspace
- Usar la versión más reciente de Google ChromeOS en el canal estable.

Para obtener más información sobre la compatibilidad con versiones anteriores, exclusiones y preguntas frecuentes, consulte la sección Compatibilidad con ChromeOS LTS de la página Instalación.

Artículos de referencia

- Global App Configuration Service
- Optimización para Microsoft Teams
- Optimización de Microsoft Teams en entornos de Citrix Virtual Apps and Desktops
- Tech Brief: Workspace Single Sign-On
- Tech Paper: Citrix Workspace app quick start guide
- Tech Brief: Citrix Workspace
- Documentación para desarrolladores: SDK de la aplicación Citrix Workspace para Chrome HDX
- Documentación para desarrolladores: Citrix Virtual Channel SDK
- Calendarios de publicación de versiones de la aplicación Citrix Workspace

Novedades de los productos relacionados

- Citrix DaaS
- Citrix Workspace
- StoreFront
- Aplicación Citrix Workspace para Windows
- Aplicación Citrix Workspace para HTML5
- Interfaz de usuario (IU) de Workspace

Documentación antigua

Para ver las versiones de productos que han alcanzado el fin de su vida (EOL), consulte Documentación antigua.

Acerca de esta versión

June 19, 2024

Conozca las nuevas funciones, las mejoras, los problemas resueltos y los problemas conocidos.

> **Nota:**
>
> ¿Busca funciones en Technical Preview? Hemos seleccionado una lista para que pueda tenerlas en un solo lugar. Explore nuestra página Funciones en Technical Preview y comparta sus comentarios mediante el enlace adjunto al formulario de Podio.

Novedades de la versión 2405

Esta versión es compatible con la versión 125 de ChromeOS. En esta versión, se trató una serie de áreas para mejorar la estabilidad y el rendimiento general.

Technical Preview

- Barra de herramientas mejorada en la sesión.

Para obtener la lista completa de las funciones en Technical Preview, consulte la página Funciones en Technical Preview.

Problemas resueltos en la versión 2405

- En una configuración de varios monitores, al abrir una aplicación publicada, se muestra una pantalla en blanco en lugar de la pantalla de la aplicación. Este problema se produce cuando se utiliza el modo H.264 de pantalla completa. Para obtener más información, consulte Limitaciones. [CVADHELP-24883]
- En los dispositivos no administrados, al iniciar una sesión de escritorio o aplicación, el nombre de cliente que se envía desde la aplicación Citrix Workspace para ChromeOS es HTML5-X-X. Tras la corrección, el nombre del cliente ahora aparece como CrOS-X-X. [RFHTMCRM-12155]
- Cuando habilita la función de continuidad del servicio e inicia una sesión sin conexión, los archivos de arrendamiento no se descargan de forma intermitente, después de cerrar sesión en Citrix Workspace y volver a iniciarla. [RFHTMCRM-12492]
- Cuando inicia una sesión de escritorio y abre una aplicación para introducir texto, al empezar a escribir, el texto desaparece y vuelve a aparecer. Puede notar que el texto parpadea. Este problema se produce cuando se utiliza el modo H.264 de pantalla completa. Para obtener más información, consulte Limitaciones. [CVADHELP-24883]

Problemas conocidos en la versión 2405

No hay nuevos problemas conocidos.

> **Nota:**
>
> - Para obtener una lista completa de los problemas de las versiones anteriores, consulte la sección Problemas conocidos.

Versiones anteriores

En esta sección se proporciona información sobre las nuevas funciones y los problemas resueltos en las versiones anteriores disponibles según lo indicado en Lifecycle Milestones for Citrix Workspace app.

2402.1

Novedades

Esta versión es compatible con la versión 121 de ChromeOS. En esta versión, se trató una serie de áreas para mejorar la estabilidad y el rendimiento general.

Compatibilidad con la optimización para Zoom A partir de la versión 2402.1, la aplicación Citrix Workspace para ChromeOS admite la integración con la solución de infraestructura de escritorio virtual (VDI) de Zoom para ofrecer una experiencia optimizada en las conferencias de audio y vídeo dentro de las sesiones.

Tras abordar las dependencias de terceros relacionadas con esta función, ahora se puede configurar y usar de forma inmediata. Los usuarios pueden aprovechar la optimización del audio y el vídeo, así como ver una disminución en el consumo de recursos del VDA durante las reuniones de Zoom dentro de la sesión de Citrix.

Para obtener más información sobre la función, consulte Compatibilidad con la optimización para Zoom.

Continuidad del servicio A partir de la versión 2402.1, la función de continuidad del servicio está inhabilitada.

> **Nota:**
>
> Si anteriormente habilitó la función de continuidad del servicio y está usando una versión anterior de la aplicación Citrix Workspace para ChromeOS, es posible que no pueda usar la continuidad del servicio. Para habilitar esta función, se recomienda actualizar la aplicación Citrix Workspace a la versión más reciente (2402.1 o posterior) y seguir las instrucciones del artículo CTX632723de Knowledge Center.
>
> Para obtener más información acerca de la configuración, consulte la documentación de Continuidad del servicio.

Herramienta de la utilidad de configuración Esta versión se ocupa de áreas que mejoran la estabilidad general de la herramienta de la utilidad de configuración. El parámetro de configuración **allowEditStoreName** está incluido en la herramienta.

Cómo acceder a la herramienta Anteriormente, la herramienta de la utilidad de configuración estaba disponible en la página Knowledge Center.

A partir de la versión 2402, puede descargar la herramienta de la utilidad de configuración desde la página de descargas de Citrix.

Virtual Channel SDK A partir de la versión 2402, Citrix Virtual Channel SDK (VCSDK) para ChromeOS cuenta con capacidades y funcionalidades que facilitan la compatibilidad de la aplicación Citrix Workspace para ChromeOS con plug-ins de terceros. Los plug-ins de terceros deben estar integrados con VCSDK. Esta gestión de las capacidades garantiza una compatibilidad sin fisuras hacia atrás y hacia delante en todas las versiones y combinaciones. Para obtener más información sobre estas funcionalidades, consulte la página de documentación para desarrolladores.

Además, se agregan API para casos con varios monitores.

Parámetro de proxy HTTP en Chromebook Si ha configurado el parámetro del proxy HTTP en su Chromebook, es posible que sus sesiones no se inicien.

Para obtener más información sobre cómo resolver el problema, consulte el artículo Parámetro de proxy HTTP en Chromebook.

Nombre abreviado de la URL del almacén Anteriormente podía ver las URL de los almacenes, pero no existía la posibilidad de agregar o modificar un nombre corto para las URL de almacén. Esta disposición dificultaba que los administradores y los usuarios recordaran las URL de almacén.

A partir de la versión 2402, para los usuarios administrados, los administradores pueden insertar un nombre de almacén personalizado junto con la URL del almacén desde la consola de administración de Google. Esta función facilita a los usuarios la identificación de los diferentes almacenes.

Para obtener más información sobre esta función, consulte Nombre abreviado de la URL del almacén.

Problemas resueltos

- Si tiene escritorios virtuales con un nombre del grupo de entrega que contiene caracteres de varios bytes, no puede iniciar una sesión de escritorio virtual. [CVADHELP-24846]

- Si está realizando una llamada de Microsoft Teams optimizado y decide dejar de compartir la pantalla, es posible que vea un rectángulo en blanco en lugar de la sección de vídeo. [RFHTMCRM-11689]
- En el modo quiosco, es posible que las sesiones no se inicien automáticamente aunque el parámetro **Inicio automático del escritorio** esté habilitado en StoreFront. [CVADHELP-23698] [RFHTMCRM-11815]
- Al habilitar la función de continuidad del servicio y hacer clic en **Reconectarse a Workspace**, en la pantalla de inicio de sesión no aparece el banner **Usar Workspace sin conexión**. [RFHTMCRM-11720]
- El icono de la aplicación Citrix Workspace se muestra en la estantería de Chrome en lugar de los iconos de la sesión de escritorio real. Este problema se produce cuando se habilita la función de continuidad del servicio y se produce la interrupción de la implementación en la nube. [RFHTMCRM-11647]
- Al copiar y pegar archivos de más de 4 KB mediante la función de asignación de unidades del cliente desde el dispositivo local al VDA, es posible que los datos se dañen. [RFHTMCRM-12156]
- Durante una sesión, es posible que los clics del mouse dejen de responder. [RFHTMCRM-11841] [CVADHELP-24210]
- Cuando un usuario cierra sesión en la página de un almacén (de forma intencionada o por inactividad) y vuelve a iniciar sesión en la misma página del almacén, es posible que la página del almacén quede en blanco o que aparezca icono giratorio infinito. Este problema se produce en las implementaciones en la nube habilitadas para continuidad del servicio. [RFHTMCRM-12212]

2312

Novedades

Esta versión es compatible con la versión 119 de ChromeOS. En esta versión, se trató una serie de áreas para mejorar la estabilidad y el rendimiento general.

Compatibilidad con timbre secundario Puede usar la función de timbre secundario para seleccionar un dispositivo secundario en el que recibir la notificación de llamada entrante cuando Microsoft Teams está optimizado.

Por ejemplo, considere que ha establecido un altavoz como timbre secundario y que su dispositivo de punto final está conectado a los auriculares. En este caso, Microsoft Teams envía el timbre de la llamada entrante tanto a los auriculares como al altavoz. No se puede establecer un timbre secundario en los siguientes casos:

- Cuando no se ha conectado a más de un dispositivo de audio
- Si el periférico no está disponible (por ejemplo, auriculares Bluetooth con micrófono)

> **Nota**
>
> De forma predeterminada, esta función está inhabilitada.

Limitaciones conocidas de la función

- Al habilitar esta función, es posible que oiga el timbre secundario dos veces con una ligera demora. Este problema es un error de Microsoft Teams, y planean solucionarlo en la próxima versión de Microsoft Teams.

Para obtener más información sobre la configuración, consulte Compatibilidad con timbre secundario.

Implementación de la transmisión simultánea para llamadas de videoconferencia de Microsoft Teams optimizado A partir de la versión 2312, la función de transmisión simultánea está habilitada de forma predeterminada para las llamadas de videoconferencia en Microsoft Teams optimizado. Con esta compatibilidad, la calidad y la experiencia de las videoconferencias en diferentes dispositivos de punto final mejoran. Esto se logra al adaptarse a la resolución adecuada para ofrecer la mejor experiencia de llamadas para todos los usuarios.

Con esta experiencia mejorada, cada usuario podría ofrecer varias transmisiones de vídeo en diferentes resoluciones en función de varios factores, como la capacidad del dispositivo de punto final, las condiciones de la red, etc. Por ejemplo, 720p, 360p, etc. El dispositivo de punto final receptor solicita entonces la resolución de máxima calidad que pueda gestionar, lo que ofrece a todos los usuarios una experiencia de vídeo óptima.

URL de almacén sin HTTPS A partir de la versión 2312, puede introducir la URL de almacén directamente sin mencionar `https://` explícitamente en la URL.

> **Nota:**
>
> Si sigues usando un almacén `http`, le recomendamos encarecidamente que migre al almacén `https`. Mientras tanto, para acceder a su almacén `http`, agregue `http` de forma explícita al principio de la URL de almacén.

Problemas resueltos

- Es posible que haya sesiones que no se inicien cuando se produce una interrupción del servicio en la implementación de la nube. Para obtener más información sobre cómo configurar la continuidad del servicio, consulte Continuidad del servicio. [RFHTMCRM-11539]

- En una sesión, al abrir la aplicación Microsoft Excel y usar la combinación de teclas **Ctrl + barra espaciadora**, es posible que la combinación de teclas no funcione como es debido. [RFHTMCRM-11718]

2311

Novedades en la versión 2311

Esta versión es compatible con la versión 119 de ChromeOS. En esta versión, se trató una serie de áreas para mejorar la estabilidad y el rendimiento general.

Technical Preview

- Transporte adaptable

Para obtener la lista completa de las funciones en Technical Preview, consulte la página Funciones en Technical Preview.

Problemas resueltos en la versión 2311

- Es posible que la redirección de USB no se realice correctamente si la directiva de DDC V1 definida en Citrix Studio en la máquina DDC no surte efecto. El problema se produce cuando la directiva de DDC V1 no se establece como una prioridad superior al parámetro del Registro de VDA que contiene la clave `\HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\PortICA\GenericUSB`. [RFHTMCRM-11072]
- Al iniciar una sesión de escritorio y consultar la consola de Citrix Director, es posible que el valor de ICARTT sea cero. Es posible que el valor de ICARTT tenga un valor positivo si lo consulta inmediatamente después de iniciar la sesión. Sin embargo, después de un tiempo, es posible que aparezca un cero. [CVADHELP-23905]

2310

Novedades

Esta versión es compatible con la versión 118 de ChromeOS. En esta versión, se trató una serie de áreas para mejorar la estabilidad y el rendimiento general.

Problemas resueltos en la versión 2310

- Al iniciar una sesión en la aplicación Citrix Workspace para ChromeOS en un Chromebook, es posible que los archivos de Google Drive no se abran. [RFHTMCRM-10540]
- Al abrir la aplicación Citrix Workspace para ChromeOS e ir a **Parámetros** > **General** > y seleccionar la opción **Escalado de PPP elevados**, es posible que vea un cursor duplicado al iniciar la sesión de escritorio. [RFHTMCRM-10839]
- Cuando use Microsoft Teams en una sesión de escritorio, es posible que el vídeo del participante no aparezca correctamente si configura la resolución de pantalla en la opción de **escalado de la proporción de píxeles del dispositivo**. [RFHTMCRM-5271]
- En una sesión, es posible que no aparezcan los dispositivos de audio, incluidos los altavoces y los micrófonos. El problema se produce si el equipo local no tiene dispositivos de micrófono o si el usuario inhabilita todos los dispositivos de micrófono. [RFHTMCRM-10900]

2309.5

Novedades

Esta versión es compatible con la versión 117 de ChromeOS. En esta versión, se trató una serie de áreas para mejorar la estabilidad y el rendimiento general.

Problemas resueltos

Esta versión aborda los problemas relacionados con la API de administración de ventanas y Virtual Channel SDK.

2309

Novedades

Esta versión es compatible con la versión 117 de ChromeOS. En esta versión, se trató una serie de áreas para mejorar la estabilidad y el rendimiento general.

Modo de entrada de texto Scancode La aplicación Citrix Workspace le permite utilizar teclados físicos externos para colaborar con la distribución del teclado del lado del servidor en el VDA. Cuando los administradores habilitan el modo Scancode, es posible que el usuario final utilice la distribución del teclado del servidor en lugar del cliente.

Esta función mejora la experiencia del usuario, especialmente cuando se usa un teclado físico en un idioma de Asia oriental.

> **Notas:**
>
> - De forma predeterminada, esta directiva de función está inhabilitada.
> - En los dispositivos táctiles, cuando la opción Scancode está habilitada, el teclado de software en pantalla no funciona desde la aplicación Citrix Workspace.

Para obtener más información sobre la configuración, consulte Modo de entrada de texto Scancode.

Asignación de teclado personalizada A partir de la versión 2309, los usuarios finales pueden usar accesos directos y combinaciones de teclas específicos de Windows cuando el VDA es una máquina con sistema operativo Windows y el dispositivo de entrada nativo es un teclado ChromeOS. Ahora puede asignar las teclas **Ctrl** y **Alt** de forma personalizada. El usuario puede seleccionar la tecla Control (Ctrl) derecha o izquierda para que actúe como tecla Alt.

> **Notas:**
>
> - Esta asignación solo es posible en el modo de pantalla completa.
> - Tras guardar la configuración, la asignación afecta a todas las sesiones.
> - Esta función está habilitada de forma predeterminada.

Para obtener más información sobre la configuración, consulte Asignación de teclado personalizada.

Para obtener más información sobre cómo utilizar la función, consulte la documentación de ayuda.

Uso de los accesos directos del sistema en el VDA en el modo de pantalla completa A partir de la versión 2309, la aplicación Citrix Workspace en los dispositivos ChromeOS permite pasar los accesos directos del sistema al VDA (sesión de escritorio remoto) en modo de pantalla completa. Sin embargo, no surte efecto en el sistema operativo del cliente.

Anteriormente, estas combinaciones funcionaban a nivel local. Ahora, cuando la función está habilitada y en modo de pantalla completa, estas combinaciones se envían al VDA, aunque no se aplican localmente. Por ejemplo, la tecla **Actualizar** es una tecla del sistema en el Chromebook, y la combinación **Ctrl+Mayús+Actualizar** es un acceso directo del sistema en ChromeOS para girar la pantalla. Sin embargo, el VDA Windows no realiza ninguna acción, puesto que no existe ese acceso directo en el sistema operativo Windows.

Otro ejemplo: `Alt+[` sirve para acoplar una ventana de ChromeOS a la izquierda, pero el mismo acceso directo no tiene ningún efecto en un VDA Windows. Algunas aplicaciones pueden usar estos accesos directos para una función específica; por ejemplo, algunos escáneres de códigos de barras usan `Alt+[` como prefijo.

> **Nota:**
>
> - Esta función está habilitada de manera predeterminada.

Para obtener más información sobre la configuración, consulte Uso de los accesos directos del sistema en el VDA en el modo de pantalla completa.

Problemas resueltos en la versión 2309

- En el modo quiosco con una configuración de varios monitores, es posible que ambas pantallas se pongan de color negro al conectar el segundo monitor e iniciar la sesión [RFHTMCRM-10905].

  Si tiene la versión 2308, le recomendamos que actualice a la versión 2309.

  Sin embargo, si quiere seguir trabajando en la versión 2308, agregue los siguientes datos de JSON desde la consola de administración de Google:

```
{

"settings": {

        "Value": {

                "settings_version": "1.0",
                "engine_settings": {

                        "features": {

                                    "graphics": {

                                    "graphicsWebWorker": {

                                                "enabled":
                                                   false
                                            }
,
                                "graphicsWasmRender": false
                                            }

                                     }

                            }

                    }

          }

 }

<!--NeedCopy-->
```


2308

Novedades en la versión 2308

Esta versión es compatible con la versión 115 de ChromeOS. Esta versión mejora el rendimiento relacionado con los gráficos.

Problemas resueltos en la versión 2308

- Al iniciar una sesión en el modo de sesión de invitado administrada, es posible que la redirección automática de USB no funcione como es debido. [RFHTMCRM-10625]
- La función de continuidad del servicio no está operativa. En otras palabras, que no puede conectarse a las aplicaciones y escritorios de DaaS durante las interrupciones del servicio. [RFHTMCRM-9261]

2307

Novedades

Esta versión es compatible con la versión 114 de ChromeOS. Además, en esta versión se han resuelto algunos problemas para mejorar la estabilidad y el rendimiento generales.

Mejoras de Microsoft Teams La optimización de Microsoft Teams admite la transcripción en tiempo real de lo que dice los ponentes cuando los subtítulos en directo están habilitados en Microsoft Teams.

Redirección automática de dispositivos USB Para redirigir dispositivos USB automáticamente, debe seguir las reglas de los dispositivos USB.
Puede configurar las reglas de los dispositivos USB mediante:

- Directiva administrativa de Google
- Reglas de dispositivo
- Reglas de redirección de dispositivos USB del cliente (versión 2)

Mejora de la experiencia en sesiones HDX Con una técnica de compresión mejorada, la aplicación Citrix Workspace para ChromeOS consume pocos recursos de red y mejora la capacidad de respuesta de las sesiones.

Mejoras en la redirección de dispositivos USB compuestos mediante directivas de DDC A partir de la versión 2307, puede determinar si una clase o interfaz de USB compuesto concreto puede redirigir al VDA de forma predeterminada o no. Si tiene un USB compuesto conectado al dispositivo ChromeOS, la configuración **enableDefaultAllowPolicy** le ayuda a decidir si, de forma predeterminada, puede permitir la redirección de USB mediante directivas de DDC. La versión 2212 de VDA y las posteriores ofrecen esta función.

Para obtener más información, consulte la documentación sobre Mejoras en la redirección de dispositivos USB compuestos mediante directivas de DDC.

Asignación de unidades del cliente A partir de la versión 2307, la función de asignación de unidades del cliente (CDM) permite la asignación de carpetas en el dispositivo ChromeOS local, lo que permite acceder a ellas desde una sesión. Puede asignar cualquier carpeta desde el dispositivo ChromeOS. Por ejemplo, carpetas de Descargas, Google Drive y unidades USB, si la carpeta no contiene archivos del sistema.

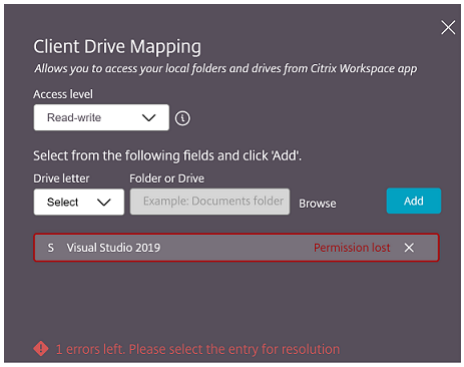
El usuario final puede realizar estas operaciones:

- Copie archivos y carpetas a la unidad asignada desde y hacia la sesión.
- Ver la lista de archivos y carpetas de la unidad asignada.
- Abra, lea y modifique el contenido de los archivos en la unidad asignada.
- Ver las propiedades de los archivos (solo la hora de la modificación y el tamaño de los archivos) en la unidad asignada.

Esta función ofrece la ventaja de acceder simultáneamente a unidades de escritorio virtuales y unidades de máquinas locales en el Explorador de archivos dentro de la sesión HDX.

Limitaciones conocidas

- No puede cambiar el nombre de archivos ni de carpetas dentro de la unidad asignada.
- Las asignaciones tienen el nombre de la carpeta, no la ruta completa.
- Si la carpeta local tiene archivos ocultos y ha asignado la misma carpeta, los archivos ocultos serán visibles dentro de la sesión en la unidad asignada.
- No puede cambiar la propiedad del archivo para que sea de solo lectura en la unidad asignada.
- CDM no está disponible cuando las sesiones se abren en modo incrustado con el SDK de HDX.
- Al asignar una carpeta de un dispositivo extraíble, si se retira el dispositivo durante una sesión activa, no se puede usar la unidad asignada dentro de la sesión. Para quitar las asignaciones manualmente, haga clic en la marca **X** que hay al lado de la asignación en cuestión.



Para obtener más información, consulte la documentación de Asignación de unidades del cliente.

Technical Preview

- Accesibilidad y TalkBack

Para obtener la lista completa de las funciones en Technical Preview, consulte la página Funciones en Technical Preview.

Problemas resueltos

- Cuando el usuario final abre una aplicación publicada y actualiza la aplicación Citrix Workspace, aparece una instancia duplicada de la aplicación publicada. Para aplicar los parámetros de configuración, consulte la sección Actualizar almacén. [CVADHELP-22229]
- En el modo de varios monitores, al abrir una aplicación publicada en el monitor secundario, es posible que los clics del mouse no se comporten como es debido. [CVADHELP-21916]
- Es posible que la ventana de notificación del progreso del inicio de la sesión que aparece en la parte inferior derecha de la pantalla no se cierre a pesar de que ya se haya iniciado la sesión. El problema se produce cuando la versión del VDA es 7.15. [RFHTMCRM-10161]

2306

Esta versión es compatible con la versión 114 de ChromeOS, que Google ha elegido como versión Long Term Support (LTS). Por ello, Citrix sigue ofreciendo asistencia y desarrollo para esta versión hasta el final de la vida útil de LTS. Consulte la Declaración de compatibilidad de Citrix para obtener información detallada sobre las exclusiones.

Novedades

Configurar la redirección de dispositivos USB compuestos mediante directivas de DDC Antes, los administradores usaban directivas de administración de Google para configurar la redirección de

USB del lado del cliente.

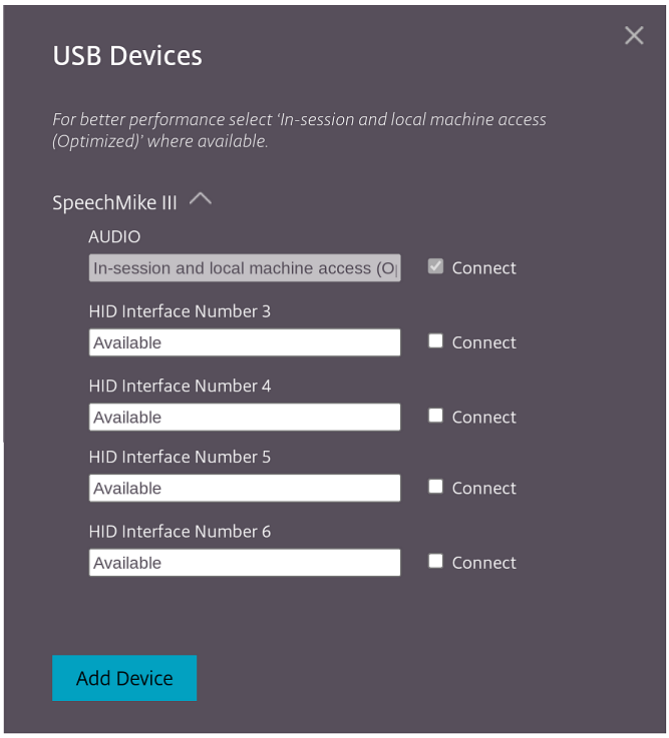
A partir de la versión 2306, también puede configurar la redirección de USB mediante las directivas de DDC. Las configuraciones mediante directivas de DDC permiten que los administradores dispongan de una forma unificada y centralizada de definir directivas y comportamientos. Estas directivas se aplican a implementaciones locales y de la nube en dispositivos y usuarios administrados. Esta función está disponible en VDA 2212 y versiones posteriores.

Para obtener información sobre la configuración, consulte la documentación en Configurar la redirección de dispositivos USB compuestos mediante directivas de DDC.

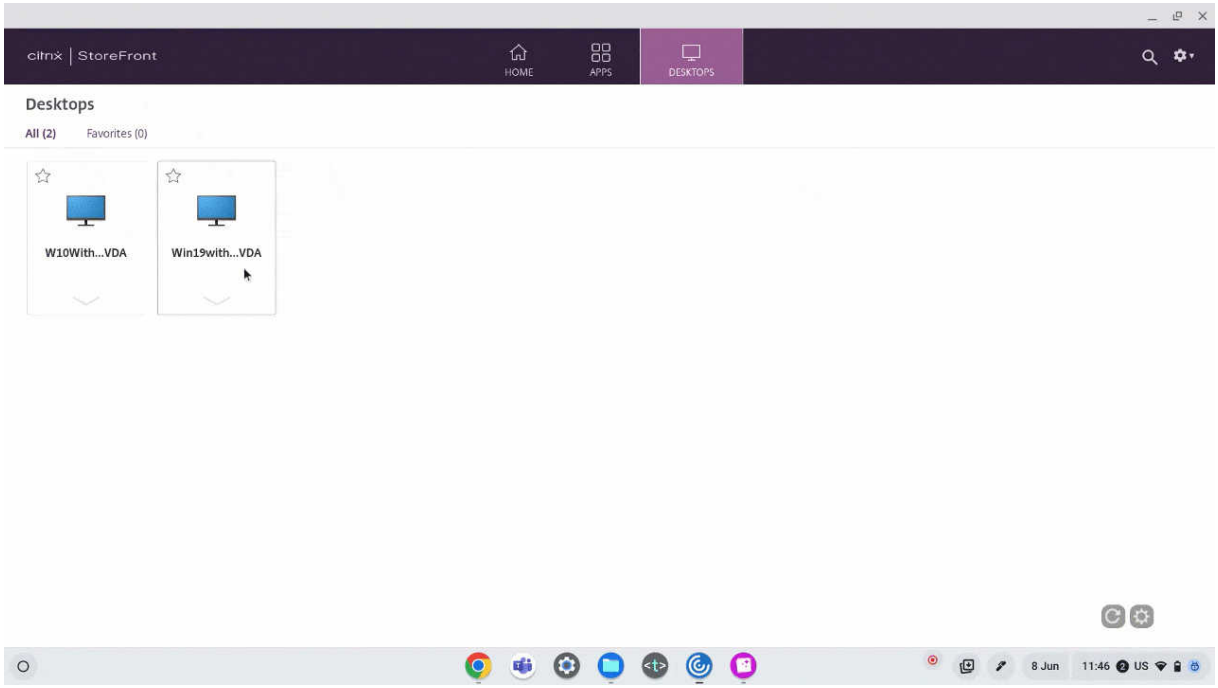
Mejoras en la interfaz de usuario de dispositivos USB compuestos A partir de la versión 2306, cuando la configuración de un dispositivo USB compuesto está definida en "split": true, la interfaz de usuario de **Dispositivos USB** muestra los componentes en función de números de la interfaz en lugar de clases de la interfaz.

Para obtener más información, consulte el artículo Redirección de dispositivos USB compuestos.

Interfaz de usuario A continuación, se muestra un ejemplo:



Experiencia mejorada al iniciar aplicaciones y escritorios virtuales A partir de la versión 2306, la experiencia mejorada en el inicio de aplicaciones y escritorios proporciona información oportuna y relevante sobre el estado del inicio.



Problemas resueltos

- Al desconectar y conectar el dispositivo USB que ya está en una sesión, se produce un error al redirigir de nuevo el dispositivo. Aparece una interfaz de usuario con un icono giratorio de carga hasta que reinicia la aplicación Citrix Workspace. [RFHTMCRM-9715]
- Cuando se encuentra en una reunión optimizada de Microsoft Teams, la transmisión de la cámara por streaming falla. El vídeo aparece borroso y, a veces, puede dejar de responder. El problema ocurre cuando la función de compartir pantalla está inhabilitada y el usuario final habilita la cámara en una reunión de Microsoft Teams. [RFHTMCRM-9968]
- En un Chromebook, cuando la sesión está en modo tableta, es posible que deba tocar el icono de la aplicación (por ejemplo, el icono del bloc de notas) varias veces desde la estantería de Chrome para centrar la aplicación integrada. [RFHTMCRM-9803]
- Cuando las sesiones están en modo tableta, es posible que el lápiz óptico del Chromebook no funcione. [RFHTMCRM-9951]
- En una sesión, es posible que los usuarios finales noten problemas de audio intermitentes. El problema ocurre tras actualizar la aplicación Citrix Workspace para ChromeOS a la versión 2304 y versiones posteriores. [CVADHELP-22784]

2305

Novedades

Compatibilidad con impresoras de red Anteriormente, la opción Citrix PDF Printer se utilizaba para imprimir desde la sesión de escritorio virtual. El controlador de impresión convertía el archivo a formato PDF y lo transfería al dispositivo local. El PDF se abría en una ventana nueva para verlo e imprimirlo.

A partir de la versión 2305, la aplicación Citrix Workspace para ChromeOS admite la impresión en red. Los usuarios finales pueden ver la lista de impresoras que están conectadas a su Chromebook dentro de la sesión. Los usuarios pueden seleccionar una impresora directamente sin generar archivos PDF intermedios en el dispositivo local. Esta función se admite en:

- VDA 2112 y versiones posteriores.
- ChromeOS 112 y versiones posteriores.

> **Nota:**
>
> - De forma predeterminada, esta función está habilitada y solo se admite el formato PDF de impresión de metarchivos.

Para obtener información sobre cómo configurar, consulte la documentación de Compatibilidad con impresoras de red.

Compatibilidad con varios almacenes A partir de la versión 2305, los administradores de TI pueden asignar varios almacenes a los usuarios finales. Ahora, es fácil para los usuarios finales cambiar entre almacenes sin necesidad de recordar su URL exacta. Esta función mejora la experiencia del usuario al acceder a varios almacenes.

Para obtener información sobre cómo configurar, consulte la documentación sobre Compatibilidad con varios almacenes.

Mejoras en la redirección de URL Anteriormente, cuando se habilitaba la [redirección de host a cliente] (/en-us/citrix-workspace-app-for-chrome/configure.html#host-to-client-redirection), las URL se interceptaban en el VDA del servidor y se enviaban al dispositivo del usuario. La aplicación Citrix Workspace para ChromeOS mostraba un cuadro de diálogo en el que se pedía al usuario que eligiera abrir la URL en la sesión o en el dispositivo local. Aparecía el cuadro de diálogo para cada URL.

A partir de la versión 2305, los administradores pueden configurar la redirección de URL para abrir los enlaces en el dispositivo local sin que aparezcan cuadros de diálogo extra. De esta forma, mejora la experiencia del usuario.

> **Nota:**
>
> - De forma predeterminada, esta función está inhabilitada.

Para obtener información sobre cómo configurar, consulte la documentación sobre Mejoras en la redirección de URL.

Compatibilidad con Manifest V3 en supuestos de SDK A partir de la versión 2305, la aplicación Citrix Workspace para ChromeOS admite que HDX SDK con extensiones de Chrome tenga Manifest versión 3.

Para obtener más información, consulte Citrix Workspace app for ChromeOS HDX SDK en la documentación para desarrolladores.

Mejoras en Virtual Channel SDK A partir de la versión 2305, la aplicación Citrix Workspace para ChromeOS admite las API de administración de ventanas en el Virtual Channel SDK. Las API web permiten a los administradores de TI crear aplicaciones interactivas y personalizarlas para sus usuarios finales.

Problemas resueltos

- Al intentar desconectar una sesión de escritorio o aplicación virtual a través de HDX SDK para ChromeOS, la sesión permanece activa en Desktop Delivery Controller. Sin embargo, el estado de la sesión cambia a inactiva después de un par de minutos. [RFHTMCRM-9181]
- En una sesión, cuando hay dos participantes en una reunión optimizada de Microsoft Teams, es posible que el uso compartido de la pantalla y el audio no funcionen como es debido. El problema se produce al activar y desactivar la cámara varias veces durante la llamada. [CVADHELP-22251]
- Al actualizar el dispositivo a la versión 108 de ChromeOS, es posible que el texto del escritorio publicado aparezca borroso. El problema ocurre en dispositivos en los que la unidad de procesamiento de gráficos (GPU) no admite una precisión media. [CVADHELP-22362]

  > **Nota:**
  >
  > - La configuración de pantalla de algunos dispositivos no admite la alta precisión y es posible que el texto en el escritorio publicado aparezca correctamente. Sin embargo, es posible que la pantalla tenga un aspecto anormal debido a esta corrección. Para corregirlo, los administradores pueden establecer el atributo **webglHighPrecision** en

> **false** a través de la directiva administrativa de Google.
> A continuación se muestra un ejemplo de datos JSON:

```
```
        "hardware" : {

            "webglHighPrecision" : false
         }
,
<!--NeedCopy--> ```
```

### 2304

#### Novedades

**Mejoras de gestos en dispositivos táctiles** A partir de la versión 2304, la aplicación Citrix Workspace mejora la experiencia del usuario final en relación con los gestos, la funcionalidad multitoque y el teclado en pantalla (modo tableta). En las sesiones de la aplicación Citrix Workspace, puede utilizar todos los gestos de multitoque habituales, como tocar, deslizar o arrastrar.

Esta es la guía de gestos:

| Para hacerlo: | En la aplicación Citrix Workspace, haga lo siguiente: |
|---|---|
| Un clic | Tocar con un dedo |
| Clic con el botón secundario | Tocar, mantener y soltar |
| Abrir el teclado en pantalla | Tocar con tres dedos (o, desde la barra de herramientas, tocar el icono **Teclado**) |
| Arrastrar | Tocar, mantener y deslizar |
| Habilitar el cursor | Tocar con dos dedos |

#### Problemas resueltos en la versión 2304

- No hay problemas resueltos en esta versión.

 
```

2303

Novedades

Esta versión es compatible con la versión 111 de ChromeOS. Además, en esta versión se han resuelto algunos problemas para mejorar la estabilidad y el rendimiento generales.

Compatibilidad con dispositivos de audio Plug and Play Antes, solo se admitía un único dispositivo de reproducción y grabación de audio, y se mostraba como **Citrix HDX Audio**, independientemente del nombre real del dispositivo.

A partir de la versión 2303, puede conectar varios dispositivos de audio y redirigirlos al VDA. Ahora, al redirigir dispositivos USB de audio, puede ver el nombre real del dispositivo de audio en **Parámetros de sonido** > **Parámetros de reproducción y sonido** > **Grabación** en el VDA. La lista de dispositivos del VDA se actualiza dinámicamente cada vez que se conecta o se quita un dispositivo de audio.

> **Nota:**
>
> De manera predeterminada, esta función está habilitada.

Para obtener más información, consulte Compatibilidad con dispositivos de audio Plug and Play.

Desenfoque de fondo y efectos en la optimización de Microsoft Teams A partir de la versión 2303, la aplicación Citrix Workspace para ChromeOS admite el desenfoque de fondo y los efectos en la optimización de Microsoft Teams para videollamadas. Puede difuminar el fondo o reemplazar los efectos de fondo proporcionados por Microsoft Teams para evitar distracciones inesperadas y ayudar a que la conversación se centre en la silueta de la persona (cuerpo y rostro). Esta función se puede utilizar con llamadas de conferencia y entre dos usuarios.

> **Notas:**
>
> - De forma predeterminada, esta función está inhabilitada.
> - Ahora, esta función está integrada en los botones y la interfaz de usuario de Microsoft Teams. La compatibilidad con varias ventanas es un requisito previo que necesita una actualización de VDA a la versión 2112 o a una posterior. Para obtener más información, consulte Reuniones y chat en modo multiventana.

Para obtener más información, consulte Desenfoque de fondo y efectos en la optimización de Microsoft Teams.

Problemas resueltos en la versión 2303

- En una sesión, cuando dos participantes están en una reunión de Microsoft Teams optimizado, la pantalla se vuelve negra cuando la cámara se inhabilita. Además, al hacer clic en iconos como Compartir pantalla, Chat o Personas, se puede hacer clic en los iconos. Sin embargo, las opciones que hay debajo se ocultan bajo la pantalla negra y no se ven como es debido. [CVADHELP-22173]

2301.1

Novedades

En esta versión se han resuelto algunos problemas para mejorar la estabilidad y el rendimiento generales.

Problemas resueltos

- Al copiar o pegar texto en la sesión, la sesión deja de responder. El problema se produce al utilizar la versión 2301 de la aplicación Citrix Workspace para ChromeOS. [CVADHELP-21951]
- La redirección de dispositivos de audio a la sesión de Citrix Virtual Apps and Desktops no funciona. Aparece una "X"roja en el icono de volumen de la bandeja del sistema. El problema se produce después de actualizar la versión 2301 de la aplicación Citrix Workspace para ChromeOS. [RFHTMCRM-8799]

2301

Novedades

Esta versión es compatible con la versión 109 de ChromeOS. Además, en esta versión se han resuelto algunos problemas para mejorar la estabilidad y el rendimiento generales.

Continuidad del servicio La continuidad del servicio elimina o reduce la dependencia de la disponibilidad de los componentes involucrados en el proceso de conexión. Puede iniciar Citrix Virtual Apps and Desktops y Citrix DaaS independientemente del estado de los servicios de la nube. En otras palabras, la continuidad del servicio le permite conectarse a las aplicaciones y escritorios de DaaS durante las interrupciones del servicio. Como requisito previo, el dispositivo debe mantener una conexión de red a una ubicación de recursos.

Para obtener más información, consulte la sección Continuidad del servicio de la documentación de Citrix Workspace.

Compatibilidad con dispositivos de audio Plug and Play Antes, solo se admitía un único dispositivo de reproducción y grabación de audio, y se mostraba como **Citrix HDX Audio**, independientemente del nombre real del dispositivo.

A partir de la versión 2301, admitimos varios dispositivos de audio y los redirigimos a VDA. Ahora, al redirigir dispositivos de audio, puede ver el nombre real del dispositivo de audio en Parámetros de **sonido** > Parámetros de **reproducción** y **sonido** > **Grabación** en el VDA. La lista de dispositivos del VDA se actualiza dinámicamente cada vez que se conecta o se quita un dispositivo de audio.

Limitaciones conocidas

- En el VDA, el nombre del dispositivo de audio integrado solo está en inglés. El problema se produce al usar dispositivos basados en ChromeOS. [RFHTMCRM-8667]

Para obtener más información, consulte la documentación de Compatibilidad con dispositivos de audio Plug and Play.

Chat y reuniones multiventana para Microsoft Teams A partir de la versión 2301, puede usar varias ventanas para chatear y reunirse en Microsoft Teams. Puede separar las conversaciones o las reuniones de varias maneras.

Para obtener información detallada sobre la función de ventana emergente, consulte Desplegar un chat en Teams.

Para solucionar problemas, consulte CTX253754.

Microsoft dejará de desarrollar las ventanas únicas en el futuro. Si usa una versión anterior de la aplicación Citrix Workspace o Virtual Delivery Agent (VDA), puede actualizarla a:

- La aplicación Citrix Workspace 2301 o una versión posterior
- VDA 2203 o una versión posterior

Redirección de contenido del explorador web La redirección de contenido del explorador web (BCR) redirige el contenido del explorador web remoto al escritorio del equipo del usuario. BCR es un explorador web sin bordes ni marcos que se ejecuta dentro de la ventana del escritorio remoto y cubre (se superpone) el área de contenido del explorador web remoto (VDA).

BCR redirige el contenido de un explorador web a un dispositivo cliente y crea un explorador web correspondiente incrustado en la aplicación Citrix Workspace. Esta funcionalidad reduce el uso de red, el procesamiento de páginas y la generación de gráficos para el dispositivo de punto final. Por tanto, mejora la experiencia del usuario cuando este visita páginas web con contenido sofisticado, especialmente aquellas páginas web que contienen HTML5 o WebRTC. Solo la ventanilla (la parte visible para el usuario en la página web) se redirige al punto final. La redirección de contenido de

explorador no redirige la interfaz de usuario (la barra de direcciones, la barra de herramientas, etc.) del explorador en el VDA.

En otras palabras, BCR ofrece la posibilidad de generar páginas web incluidas en la lista de permitidos en el lado del cliente. Esta función utiliza la aplicación Citrix Workspace para crear una instancia de motor de generación correspondiente en el lado del cliente, que obtiene el contenido HTTP y HTTPS a partir de la URL.

> **Nota:**
>
> - BCR es compatible con las versiones 2212 y posteriores de Citrix Virtual Apps and Desktops.

Para obtener más información sobre cómo configurar la lista de permitidos, consulte:

- Extensión de Chrome de redirección de contenido de explorador web.
- Configuración de directiva Redirección de contenido de explorador web.

Problemas conocidos de la función

- Durante el uso de BCR, al abrir un enlace a un sitio web en una ficha nueva, este se abre en el explorador web del cliente en lugar de abrirse en el explorador web de la sesión. [HDX-43206]

Limitaciones conocidas de la función

- Esta función no admite:
  - Casos de obtención en el servidor y generación en el cliente.
  - Servidores web de autenticación integrada de Windows (IWA).
  - Función de varios monitores.
- Al cargar o descargar archivos en algunos de los sitios web redirigidos por BCR, aparece el selector de archivos de ChromeOS en lugar del selector de archivos de la sesión de VDA. [HDX-43207]
- No se admite la impresión desde páginas redirigidas por BCR.

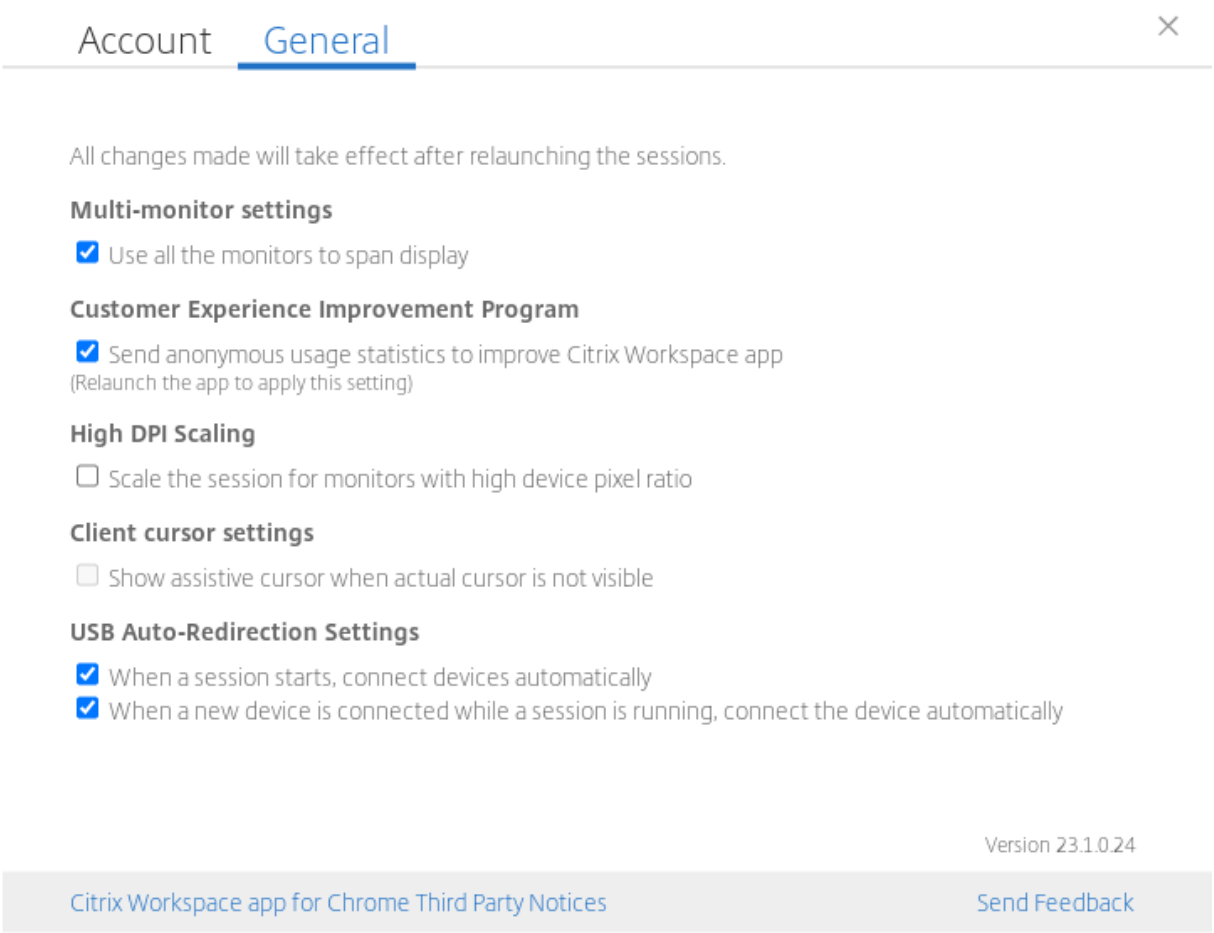
Doble salto A partir de la versión 2301, la aplicación Citrix Workspace admite casos de doble salto. Esta función es una mejora de la redirección de USB.

Para obtener más información, consulte Doble salto en la documentación de Citrix Virtual Apps and Desktops.

Parámetros de la redirección automática de USB Antes, no había ninguna opción relacionada con los parámetros de redirección automática de USB para configurar las preferencias del usuario final. Como los administradores controlan estas directivas, el usuario final tiene que redirigir manualmente los dispositivos USB necesarios en el inicio de cada sesión.

A partir de la versión 2301, el usuario final puede seleccionar una preferencia de redirección automática para cualquier dispositivo USB dentro de una sesión de Virtual Desktops. Ahora, la aplicación Citrix Workspace proporciona parámetros al nivel de la aplicación, donde el usuario final puede controlar la redirección automática de USB. El usuario final puede establecer sus preferencias y guardar los parámetros para los siguientes inicios de sesión.

Hay dos opciones: una al iniciar las sesiones y otra mientras la sesión está en curso.



Nota:

- Esta función admite implementaciones locales y en la nube, y solo está disponible para usuarios de Chrome administrados.

Problemas resueltos en la versión 2301

- En implementaciones de la nube, la función de impresión de PDF mejorada no funciona como se esperaba. La vista previa de impresión se abre en una ventana nueva en lugar de abrirse en la misma ventana. [RFHTMCRM-8672]
- La redirección de la cámara web no funciona cuando utiliza la versión 2206 y versiones posteriores de Citrix Virtual Apps and Desktops. Con la corrección más reciente, la redirección de la cámara web se realiza correctamente desde la versión 2301 de la aplicación Citrix Workspace para ChromeOS y versiones posteriores. [RFHTMCRM-8580]
- Al utilizar la versión 2203 y versiones posteriores de Citrix Virtual Apps and Desktops, es posible que la sesión de VDA aparezca distorsionada. [RFHTMCRM-8657]
- Al usar un Chromebook e intentar llamar desde Microsoft Teams optimizado, la llamada no funciona como es debido. Aparece el siguiente mensaje de error:

  "Sorry, it wasn't possible to connect". [CVADHELP-21670] [CVADHELP-21500]

Problemas conocidos

Problemas conocidos en la versión 2402.1

- Es posible que la función de continuidad del servicio no funcione para las URL de dominio personalizadas. [RFHTMCRM-12363]
- Si intenta descargar archivos o modificar archivos dentro de la unidad asignada desde un VDA mediante aplicaciones que dependen de archivos temporales, es posible que los datos se dañen. Por ejemplo, exploradores web o aplicaciones de Microsoft Office como Excel. [RFHTMCRM-12156] [RFHTMCRM-11474]
- En una sesión, es posible que note una calidad de audio deficiente. El tono de la transmisión de audio podría cambiar automáticamente.

  Como solución alternativa, establezca el atributo **AudioRedirectionV4** en **false**. Para ver los pasos detallados sobre cómo inhabilitar **AudioRedirectionV4**, consulte la sección Compatibilidad con dispositivos de audio Plug and Play. [CVADHELP-24722]

Problemas conocidos en la versión 2402

- Si intenta descargar archivos o modificar archivos dentro de la unidad asignada desde un VDA mediante aplicaciones que dependen de archivos temporales, es posible que los datos se dañen. Por ejemplo, exploradores web o aplicaciones de Microsoft Office como Excel. [RFHTMCRM-12156] [RFHTMCRM-11474]

- Cuando un usuario cierra sesión en la página de un almacén (de forma intencionada o por inactividad) y vuelve a iniciar sesión en la misma página del almacén, es posible que la página del almacén quede en blanco o que aparezca icono giratorio infinito. El problema se produce en las implementaciones en la nube que permiten la continuidad del servicio.

  Como solución alternativa, haga clic en el icono **Recargar** en la página del almacén. [RFHTMCRM-12212]

- En una sesión, es posible que note una calidad de audio deficiente. El tono de la transmisión de audio podría cambiar automáticamente.

  Como solución alternativa, establezca el atributo **AudioRedirectionV4** en **false**. Para ver los pasos detallados sobre cómo inhabilitar **AudioRedirectionV4**, consulte la sección Compatibilidad con dispositivos de audio Plug and Play. [CVADHELP-24722]

Problemas conocidos en la versión 2312

- Al habilitar la función de continuidad del servicio y cuando hay una interrupción del servicio en la implementación de la nube, el icono de la aplicación Citrix Workspace aparece en la estantería de Chrome en lugar de los iconos de la sesión de escritorio o aplicación. [RFHTMCRM-11647]

Problemas conocidos en la versión 2310

- Al iniciar una sesión de escritorio con la aplicación Citrix Workspace, aparecen bloques verdes en la pantalla que bloquea la interfaz de usuario. El problema puede producirse al mover la ventana de una aplicación dentro del escritorio iniciado. [CVADHELP-23377]
- En el modo quiosco, es posible que las sesiones no se inicien automáticamente. [CVADHELP-23698]

Problemas conocidos en la versión 2309

- En los dispositivos Chromebook, la aplicación Citrix Workspace no recurre a IPv4 desde IPv6 en una red Wi-Fi de doble pila. [CVADHELP-22537]

Problemas conocidos en la versión 2203

- Es posible que la redirección de cámara web no funcione en algunas instancias de Citrix Virtual Apps and Desktops o XenDesktop. [HDX-39396]

Limitaciones

- La aplicación Citrix Workspace para ChromeOS no admite el modo de gráficos H.264 de pantalla completa para varios monitores.
- Durante el uso compartido de la pantalla mediante la optimización de Microsoft Teams, el borde rojo de la ventana compartida no aparece.
- Al **habilitar** en Citrix Studio **Usar codificación por hardware para códec de vídeo**, es posible que la pantalla se ponga de color verde durante una sesión a través de un VDA con GPU virtual de Intel. [RFHTMCRM-5521]
- En sesiones de varios monitores a través de un VDA con Microsoft Windows 7, es posible que los monitores extendidos se vean de color negro. Además, es posible que el cursor del mouse no se genere correctamente. Recomendamos seleccionar una resolución de pantalla combinada de menos de 4800 píxeles de ancho y alto. [RFHTMCRM-5539]
- El servidor recurre a YUV420 incluso aunque esté configurado con el parámetro YUV444 de Gráficos - Thinwire. Las aplicaciones cargadas de gráficos están limitadas al rango YUV420. [RFHTMCRM-5520]
- No se admite Single Sign-On (SSO) con el IdP (proveedor de identidades) de Google.
- Al intentar iniciar sesión en la aplicación Citrix Workspace, puede encontrar problemas al iniciar sesión. Aparece este mensaje de error: ERR_TOO_MANY_REDIRECTS.

  El problema se produce cuando utiliza el IdP de Google. [CVADHELP-19362]
- En videollamadas de Microsoft Teams optimizado, al agregar un tercer participante, el vídeo se queda vacío para uno de los dos primeros participantes. El problema se produce cuando los dos primeros participantes usan ChromeOS y el tercer participante usa un sistema operativo diferente. [RFHTMCRM-7408]
- Cuando conecta varios dispositivos de audio en una sesión, solo puede oír el audio de un dispositivo. Es posible que no pueda cambiar al otro dispositivo de audio. [HDX-49312]
- En una sesión, es posible que no oiga el audio de algunas aplicaciones al desconectarse de la sesión anterior y al conectarse a ella de nuevo a través de la barra de herramientas. [HDX-49313]
- Cuando los usuarios finales inician sesión en el almacén configurado a través de Imprivata como proveedor de identidades (IdP), aparece la pantalla de detección de clientes. Sin embargo, cuando los usuarios hacen clic en **Detectar aplicación Citrix Workspace**, aparece este error:

  "Receiver links are blocked".

  Como solución temporal, cargue de nuevo la aplicación Citrix Workspace para ChromeOS. [CVADHELP-22026]

- Cuando cambia de red y una de las conexiones Wi-Fi no tiene conexión a Internet, la función de fiabilidad de la sesión no funciona correctamente. [RFHTMCRM-12349]
- El temporizador de sincronización de archivos de concesión se restablece cada vez que hace clic en el botón de recarga de la aplicación Citrix Workspace. Esta acción afecta a las prestaciones de la función de continuidad del servicio para el usuario final. [RFHTMCRM-12499]
- Los archivos de concesión no se descargan después de cerrar sesión y volver a iniciar sesión en la aplicación Citrix Workspace para ChromeOS. [RFHTMCRM-12492]
- La función de continuidad del servicio no está disponible en el modo quiosco. [RFHTMCRM-12518]

Elementos retirados

Para obtener información sobre los elementos retirados, consulte la página Elementos retirados.

Documentación antigua

Para ver las versiones de productos que han alcanzado el fin de su vida (EOL), consulte Documentación antigua.

Technical Preview

Las funciones en versión Technical Preview están disponibles para uso en entornos de producción limitados o en entornos que no son de producción, y para dar a los clientes la oportunidad de compartir comentarios. Citrix no acepta casos de asistencia para funciones en Technical Preview, pero agradece comentarios para mejorarlas. Es posible que Citrix actúe a partir de los comentarios en función de su gravedad e importancia.

Funciones en Technical Preview

June 18, 2024

Las funciones en versión Technical Preview están disponibles para uso en entornos de producción limitados o en entornos que no son de producción, y para dar a los clientes la oportunidad de compartir comentarios. Citrix no acepta casos de asistencia para funciones en Technical Preview, pero agradece comentarios para mejorarlas. Es posible que Citrix actúe a partir de los comentarios en función de su gravedad e importancia.

Lista de funciones en Technical Preview

En esta tabla se enumeran las funciones en Technical Preview. Se trata de adelantos de funciones disponibles previa solicitud. Para habilitar cualquiera de estas funciones y enviar comentarios sobre las mismas, rellene los formularios correspondientes.

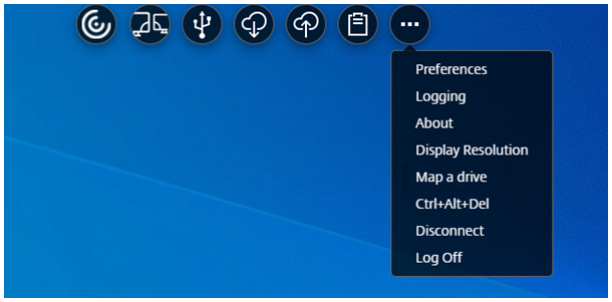
Título	Disponible a partir de la versión	Formulario de habilitación (haga clic en el icono)	Formulario de comentarios (haga clic en el icono)
Barra de herramientas mejorada en la sesión	2405	Puede configurar la función	
Transporte adaptable	2311		
Accesibilidad y TalkBack	2307	No se requiere habilitación	

Barra de herramientas mejorada en la sesión

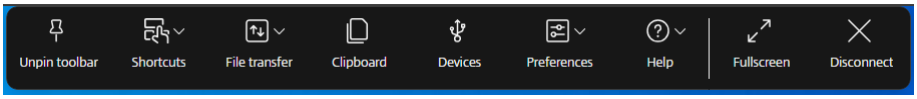
Esta función se encuentra en una Technical Preview de la versión 2405.

A partir de la versión 2405, se muestra una interfaz de usuario de barra de herramientas mejorada al iniciar una sesión de escritorio. La apariencia de la interfaz de usuario de la barra de herramientas en la sesión ha cambiado. La interfaz de usuario de la barra de herramientas está diseñada específicamente para mejorar la experiencia del usuario final al organizar las opciones de forma sencilla.

Interfaz de usuario de la barra de herramientas antigua



Interfaz de usuario de la barra de herramientas nueva



> **Nota:**
>
> Esta función está inhabilitada de forma predeterminada. Para habilitar esta función, siga los pasos de configuración. Para enviar comentarios sobre esta función, haga clic en el formulario de Podio.

Configuración

Puede habilitar la nueva interfaz de usuario de la barra de herramientas mediante la directiva administrativa de Google.

Directiva administrativa de Google Para los usuarios y dispositivos administrados, los administradores pueden habilitar la función mediante la directiva administrativa de Google de esta manera:

1. Inicie sesión en la directiva administrativa de Google.
2. Vaya a **Administración de dispositivos** > **Administración de Chrome** > **Configuración de usuario**.
3. Agregue estas cadenas al archivo **policy.txt** en la clave **engine_settings**.

   > **Nota:**
   >
   > También puede aplicar esta configuración en lo siguiente:
   >
   > - **Dispositivo** > **Chrome** > **Aplicaciones y extensiones** > **Usuarios y exploradores** > busque la extensión > Política de extensiones.
   > - **Dispositivo** > **Chrome** > **Aplicaciones y extensiones** > **Quioscos** > Buscar la extensión > Política de extensiones.
   > - **Dispositivo** > **Chrome** > **Aplicaciones y extensiones** > **Sesiones de invitados gestionadas** > Buscar la extensión > Política de extensiones.

   A continuación se muestra un ejemplo de datos JSON:

```
{

    "engine_settings": {

        "ui": {

```



```
            "toolbar":
                {
  "switchToNewToolbar": true
                }

              }

        }

 }

<!--NeedCopy-->
```

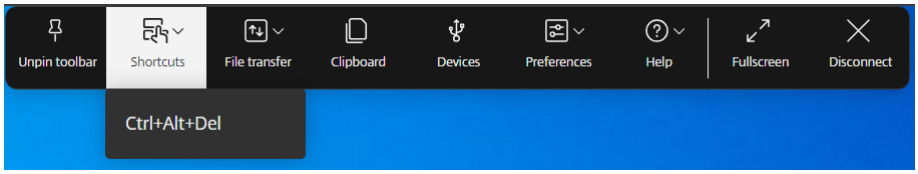
4. Guarde los cambios.

Iconos y acciones

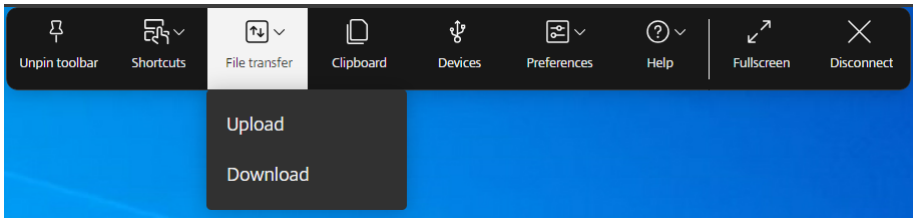
Los usuarios finales pueden realizar las siguientes acciones:

> **Nota:**
>
> Los usuarios finales solo pueden ver los iconos si el administrador de su organización ha habilitado la función específica.

- **Muesca en la barra de herramientas**: al iniciar una sesión de escritorio o aplicación, la muesca de la barra de herramientas se muestra en la parte superior de la pantalla. Al hacer clic en la muesca, la barra de herramientas se muestra sin anclar. Arrastre y cambie la posición de la muesca de la barra de herramientas a cualquier lado de la pantalla. Tras soltar el mouse, la muesca se alineará automáticamente con el borde más cercano.
- **Anclar**: al anclarla, puede arrastrar y volver a colocar la barra de herramientas en cualquier lado de la pantalla. Tras soltar el mouse, la muesca se alineará automáticamente con el borde más cercano. La ventaja de anclar la barra de herramientas es que no se minimiza y se convierte en una muesca después de completar una acción que implique iconos de la barra de herramientas.
- **Desanclar**: al desanclar la barra de herramientas, se minimiza y se convierte en una muesca tras completar una acción que implique iconos de la barra de herramientas.
- **Teclas de acceso directo**: puede ejecutar la función **Ctrl+Alt+Supr** con solo hacer clic en un botón. Esta opción facilita a los usuarios cerrar sesión, cambiar de usuario, bloquear el sistema o acceder al Administrador de tareas.



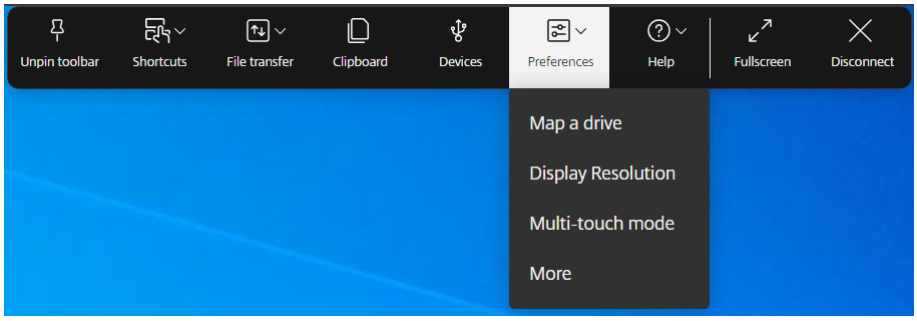
- **Transferencia de archivos**: puede cargar o descargar un archivo entre un dispositivo de usuario y una sesión. Para obtener más información, consulte Gestión de archivos.



- **Portapapeles**: puede usar la opción Portapapeles para copiar y pegar texto sin formato y datos HTML del VDA en el dispositivo local y viceversa. Para obtener más información, consulte Portapapeles.
- **Dispositivos**: haga clic para abrir el cuadro de diálogo **Dispositivos USB**. Haga clic en **Agregar** para ver los dispositivos USB conectados al dispositivo local. El cuadro de diálogo enumera los dispositivos que se pueden redirigir a la sesión. Para redirigir los dispositivos USB, seleccione un dispositivo apropiado y haga clic en **Conectar**. Para obtener más información, consulte Redirección de dispositivos USB.

  > **Nota:**
  >
  > Puede ver el icono **Dispositivos** solo si el administrador de TI proporciona acceso para conectar dispositivos USB a través de configuraciones de directivas.

- **Preferencia**: puede establecer su preferencia de la siguiente manera. Se mostrarán las siguientes opciones:

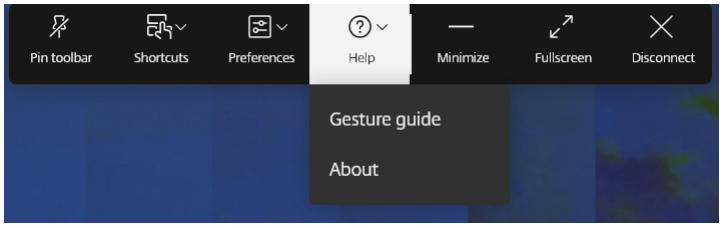


  - **Asignar una unidad**: la función de asignación de unidades de cliente (CDM) le permite acceder a las carpetas y unidades locales desde la aplicación Citrix Workspace. Para obtener más información, consulte Gestión de archivos.
  - **Resolución de pantalla**: seleccione el tamaño de la resolución para la visualización de la sesión. De forma predeterminada, la resolución de pantalla se establece en Ajuste automático de pantalla.
  - **Modo multitoque**: haga clic para usar el modo multitoque. Puede alternar entre el modo Panorámico y Multitoque. Esta opción se aplica a los dispositivos con pantalla táctil. Para

obtener más información, consulte Uso táctil y móvil.

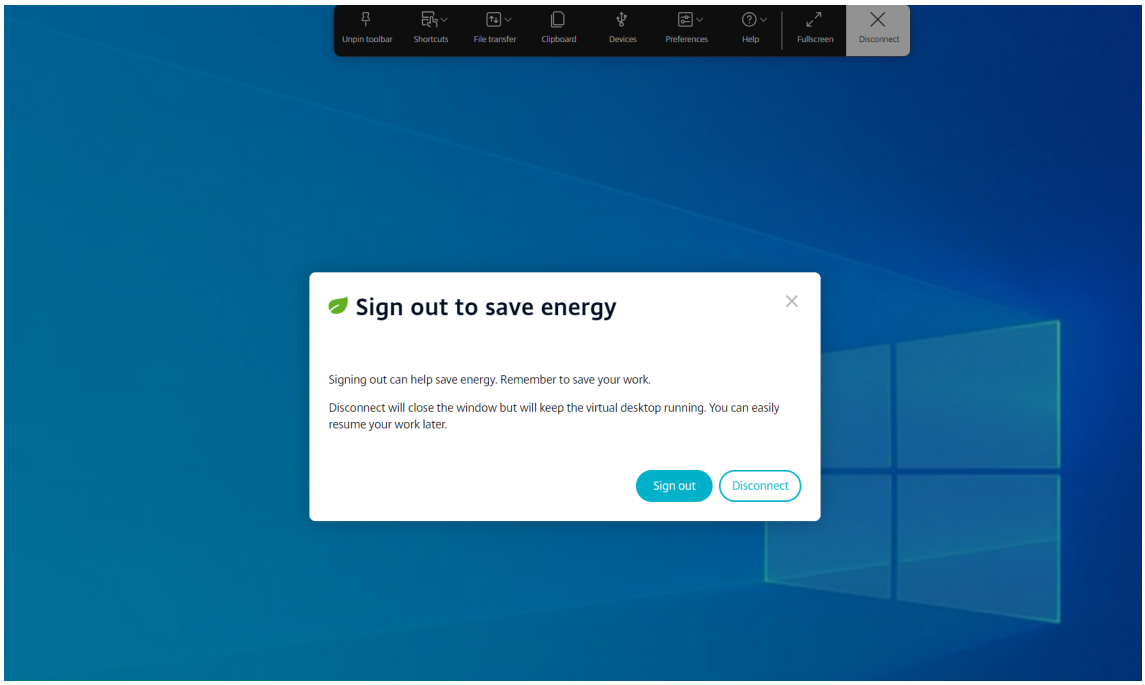
- **Más**: muestra las preferencias acerca del botón del teclado virtual y el Customer Experience Improvement Program (CEIP) de Citrix.

- **Ayuda**: se muestran las tres opciones siguientes:



  - **Guía de gestos**: se muestra una guía de gestos con detalles sobre el uso de los dedos. Esta opción se aplica a los dispositivos con pantalla táctil.
  - **Acerca de**: muestra la versión actual de la aplicación Citrix Workspace que está utilizando.

- **Minimizar**: puede minimizar la ventana de sesión.
- **Pantalla completa**: puede cambiar la pantalla de ventana a pantalla completa. Si tiene una configuración con varios monitores, el botón de pantalla completa extenderá la pantalla a lo largo de la configuración y también funcionará como un botón para varios monitores.
- **Desconectar**: la acción de desconectar mantendrá el escritorio virtual en funcionamiento. Cerrar sesión para ahorrar energía. Para obtener más información, consulte Iniciativa de sostenibilidad de la aplicación Citrix Workspace.



Transporte adaptable

Esta función se encuentra en una Technical Preview de la versión 2311.

A partir de la versión 2311, la aplicación Citrix Workspace para ChromeOS admite la función de transporte adaptable.

El transporte adaptable ofrece una experiencia de usuario superior en complicadas conexiones de larga distancia al tiempo que mantiene la escalabilidad de los servidores. Esta función ofrece una experiencia de HDX de alta calidad en plataformas basadas en web.

Para obtener más información, consulte la sección Transporte adaptable en la documentación de Citrix Virtual Apps and Desktops.

> **Notas:**
>
> - Esta función está inhabilitada de forma predeterminada.
> - Esta función se halla en una versión Tech Preview únicamente accesible mediante solicitud. Para habilitarla en su entorno, complete el formulario de Podio.

Requisitos del sistema

A continuación se detallan los requisitos para utilizar el transporte adaptable y EDT:

- Plano de control
  - Citrix DaaS (antes denominado Citrix Virtual Apps and Desktops Service)
  - Citrix Virtual Apps and Desktops 1912 o versiones posteriores.
- Virtual Delivery Agent
  - Versión 1912 o una posterior (se recomienda 2203 o una posterior)
  - La versión 2012 es la mínima necesaria para utilizar EDT con Citrix Gateway Service
- StoreFront
  - Versión 3.12.x
  - Versión 1912.0.x
- Citrix Gateway (ADC)
  - 13.1.17.42 o una versión posterior (recomendado)
  - 13.0.52.24 o una versión posterior
  - 12.1.56.22 o una versión posterior

- Firewall (desde la perspectiva del VDA)

  UDP 1494 entrante: Si la fiabilidad de la sesión está inhabilitada

  UDP 2598 entrante: Si la fiabilidad de la sesión está habilitada

  UDP 443 entrante: Si habilita el SSL del VDA para el cifrado ICA (DTLS)

  UDP 443 saliente: Si utiliza Citrix Gateway Service Para obtener más información, consulte la documentación de Citrix Gateway Service.

Configuraciones de administrador

- Para configurar el parámetro **Transporte adaptable de HDX** en la directiva de Citrix, consulte la sección Configuración de la documentación de Citrix Virtual Apps and Desktops.
- Puede configurar la función de transporte adaptable de esta manera:

  Directiva administrativa de Google

  Para los usuarios y dispositivos administrados, los administradores pueden habilitar la función mediante la directiva administrativa de Google de esta manera:

  1. Inicie sesión en la directiva administrativa de Google.
  2. Puede aplicar esta configuración a lo siguiente:
     - **Dispositivo** > **Chrome** > **Aplicaciones y extensiones** > **Usuarios y exploradores** > busque la extensión > Política de extensiones.
     - **Dispositivo** > **Chrome** > **Aplicaciones y extensiones** > **Quioscos** > Buscar la extensión > Política de extensiones.
     - **Dispositivo** > **Chrome** > **Aplicaciones y extensiones** > **Sesiones de invitados gestionadas** > Buscar la extensión > Política de extensiones.

     A continuación se muestra un ejemplo de datos JSON:

```
{

"settings": {

"Value": {

    "settings_version": "1.0",
            "engine_settings": {

                "features": {

                    "edt": {

                        "enabled": true
```

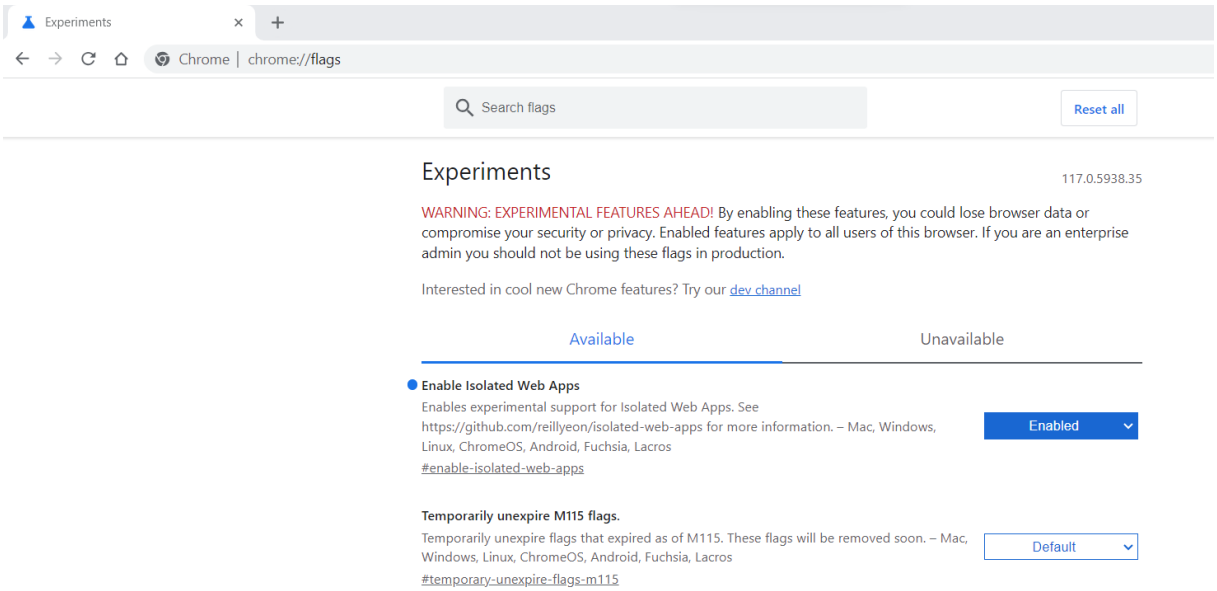


```
                                    }

                                }

                            }

                        }

                    }

    }

<!--NeedCopy-->
```

3. Guarde los cambios.

Configuración para usuarios finales

Para habilitar la función de transporte adaptable, introduzca `chrome://flags` en la barra de direcciones del explorador web Google Chrome. Habilite la opción **Habilitar aplicaciones web aisladas** tal y como se muestra en esta captura de pantalla:



Accesibilidad y TalkBack

Esta función se encuentra en una versión preliminar técnica de la versión 2307.

La aplicación Citrix Workspace ofrece una experiencia de usuario mejorada con la función TalkBack. La función TalkBack ayuda a los usuarios finales que tienen dificultades para ver la pantalla. La narración lee los elementos de la pantalla en voz alta cuando usa la interfaz de usuario.

Para usar la narración de ChromeOS (ChromeVox), los usuarios finales deben usar la combinación de teclas Ctrl+Alt+Z para encender la narración. Use la misma combinación de teclas para apagar la narración.

> **Nota:**
>
> - De forma predeterminada, esta función está inhabilitada.

Configuración

Puede configurar la función de accesibilidad de una de estas maneras:

- Configuration.js
- Directiva administrativa de Google

Configuration.js Para habilitar la función de accesibilidad mediante el archivo **configuration.js**, haga lo siguiente:

1. Busque el archivo **configuration.js** en la carpeta **raíz de ChromeApp**.

   > **Notas:**
   >
   > - Citrix recomienda hacer una copia de seguridad del archivo **configuration.js** antes de hacer cambios.
   > - Citrix recomienda modificar el archivo **configuration.js** solo si la aplicación Citrix Workspace para ChromeOS se reempaqueta para los usuarios.
   > - Se requieren credenciales de nivel de administrador para modificar el archivo **configuration.js**.

2. Modifique el archivo **configuration.js** y agregue el atributo **accessibility**. Establezca el atributo **enable** en **true**.

   A continuación se muestra un ejemplo de datos JSON:

   ```
   'features' :
   {

       'accessibility': {

             'enable': true
            }
    ,
    }


   <!--NeedCopy-->
   ```

3. Guarde los cambios.

Directiva administrativa de Google Para los usuarios y dispositivos administrados, los administradores pueden habilitar la función mediante la directiva administrativa de Google de esta manera:

1. Inicie sesión en la directiva administrativa de Google.
2. Vaya a **Administración de dispositivos > Administración de Chrome > Configuración de usuario**.
3. Agregue estas cadenas al archivo policy.txt en la clave engine_settings.
   A continuación se muestra un ejemplo de datos JSON:

```
'features' :
{

    'accessibility': {

          'enable': true
         }
 ,
 }


<!--NeedCopy-->
```

4. Guarde los cambios.

Requisitos previos para la instalación

May 16, 2024

Requisitos del sistema y compatibilidad

Requisitos

Todos los dispositivos deben cumplir los requisitos mínimos de hardware para el sistema operativo instalado.

Los dispositivos de los usuarios requieren el sistema operativo (SO) más reciente de Google Chrome para acceder a escritorios y aplicaciones mediante la aplicación Citrix Workspace. Citrix recomienda utilizar la aplicación Citrix Workspace más reciente del canal estable de Google ChromeOS.

La aplicación Citrix Workspace para ChromeOS solo se admite en ChromeOS. La aplicación Citrix Workspace también es compatible con el sistema operativo ChromeOS Flex.

Agregar y abrir aplicaciones de Chrome La aplicación Citrix Workspace para ChromeOS solo se admite en ChromeOS. En su Chromebook, puede agregar y abrir aplicaciones desde Chrome Web Store. Para obtener más información, consulte el artículo de asistencia técnica de Google.

> **Notas:**
>
> - Las aplicaciones para Chrome de Chrome Web Store solo son compatibles con dispositivos Chromebook y no funcionarán en Windows, Mac o Linux a partir de diciembre de 2022.
> - Los dispositivos Chromebook al final de su vida útil (EOL) no se actualizan a versiones más recientes de Google ChromeOS. Dichos dispositivos no admiten todas las actualizaciones de la aplicación Citrix Workspace para ChromeOS. Recomendamos y admitimos las versiones más recientes del sistema operativo de Google Chrome.

Tabla de compatibilidad

La aplicación Citrix Workspace para ChromeOS permite acceder a escritorios y aplicaciones a través de las siguientes versiones de StoreFront. El acceso a los almacenes debe hacerse mediante sitios de Citrix Receiver para Web. La aplicación Citrix Workspace para ChromeOS no ofrece el acceso directo a almacenes de StoreFront, ya sea mediante la URL del almacén o mediante la URL de los servicios XenApp.

- StoreFront 2.5 (o versiones posteriores)

La aplicación Citrix Workspace para ChromeOS se puede usar para acceder a escritorios y aplicaciones entregados a través de las siguientes versiones de producto:

- XenApp y XenDesktop 7.6 y versiones posteriores

Conexiones de usuario seguras

En un entorno de producción, Citrix recomienda proteger las comunicaciones entre los sitios de Citrix Workspace para Web y los dispositivos de los usuarios con Citrix Gateway y HTTPS. Citrix recomienda usar certificados SSL con un tamaño de clave mínimo de 1024 bits en todo el entorno en el que se implementa la aplicación Citrix Workspace para ChromeOS. La aplicación Citrix Workspace para ChromeOS permite el acceso de los usuarios a escritorios y aplicaciones desde redes públicas con las siguientes versiones de Citrix Gateway.

- NetScaler Gateway 10.5 y versiones posteriores

La aplicación Citrix Workspace para ChromeOS permite a CloudBridge inhabilitar la compresión y la compresión de impresoras, así como el uso de análisis de HDX Insight para mostrarlos en CloudBridge Insight Center.

- CloudBridge 7.4 y versiones posteriores

> **Nota:**
>
> Si no puede conectarse al VDA habilitado para SSL con la aplicación Citrix Workspace para ChromeOS, consulte Parámetros de TLS en agentes VDA. Configure el conjunto de cifrado que más le convenga.

Requisitos de la optimización de Microsoft Teams

Versión mínima:

- La optimización de Microsoft Teams para llamadas de audio, vídeo y pantalla compartida está disponible de forma general a partir de la versión 2105.5.

  Le recomendamos usar la versión más reciente de la aplicación Citrix Workspace para ChromeOS. De forma predeterminada, el uso compartido de la pantalla está inhabilitado Para habilitar el uso compartido de la pantalla, consulte Parámetros.

- Versión 1906 de VDA o una posterior.

Hardware:

Para videoconferencias entre dos usuarios pares o compartir la pantalla, los requisitos mínimos son:

- Un procesador Intel® Core™ i3 con una CPU de cuatro núcleos a 2,4 GHz que admita una resolución HD de 720p.

Instalación

May 16, 2024

Tanto los usuarios finales como los administradores de TI pueden instalar la aplicación Citrix Workspace para ChromeOS.

Instalación desde Chrome Web Store

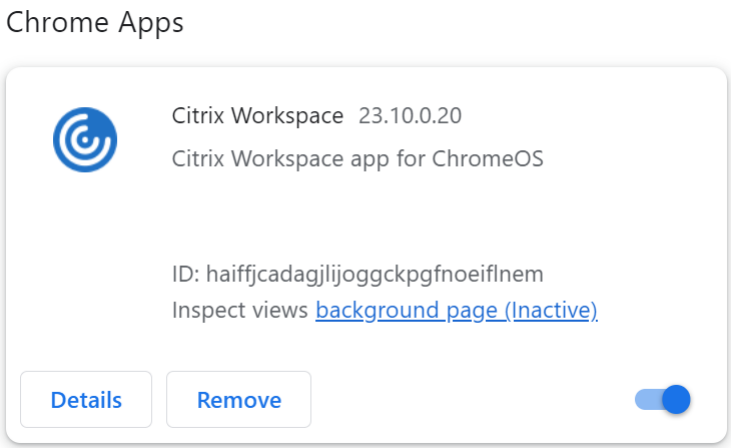
El usuario final puede instalar la aplicación Citrix Workspace para ChromeOS desde Chrome Web Store de esta manera:

1. Haga clic en el enlace https://chromewebstore.google.com/detail/citrix-workspace/haiffjcadagjlijoggckpgfnoeiflnem.

   Aparece la página de la aplicación Citrix Workspace para ChromeOS de Chrome Web Store.

2. Haga clic en **Agregar a Chrome**.

   La aplicación se instala. Vaya a `chrome://extensions` en su explorador web Chrome para ver las aplicaciones de Chrome.

3. Busque la *aplicación Citrix Workspace* en ChromeOS Launcher para usarla.

> **Nota**
>
> Para empezar a usar la aplicación, los usuarios finales pueden introducir una URL de almacén o una dirección de correo electrónico que sean válidas. Por lo general, un administrador de TI le proporciona la dirección URL de almacén o configura su dirección de correo electrónico con las URL de almacén asociadas. Siga las directrices de su organización.

Instalación manual

Hay varias opciones para implementar la aplicación Citrix Workspace para ChromeOS.

- Puede usar la consola de administración de Google Apps para configurar Citrix Workspace con una directiva de Google. Para obtener más información sobre la configuración de ChromeOS, consulte el artículo CTX141844 de Knowledge Center.
- Puede reempaquetar la aplicación Citrix Workspace para ChromeOS para incluir un archivo de configuración (CR) de la aplicación Citrix Workspace que usted haya generado previamente. El archivo **CR** contiene los datos de conexión de Citrix Gateway y del sitio de Citrix Receiver para Web que proporciona los escritorios y las aplicaciones de los usuarios. Los usuarios deben ir a chrome://extensions y, a continuación, arrastrar el archivo de la aplicación reempaquetada (CRX) y colóquelo en la ventana de Chrome para instalar la aplicación Citrix Workspace para

ChromeOS. Como la aplicación está preconfigurada, los usuarios pueden empezar a trabajar con la aplicación Citrix Workspace nada más instalarla, sin pasos de configuración adicionales.

Los administradores pueden entregar su versión personalizada de la aplicación Citrix Workspace para ChromeOS a los usuarios finales de estas maneras:

- Publique la aplicación reempaquetada para los usuarios a través de Google Apps for Business desde la Consola de administración de Google.
- Proporcione el archivo CRX a los usuarios por otros medios, como, por ejemplo, por correo electrónico.
- Los usuarios pueden instalar la aplicación Citrix Workspace para ChromeOS desde Chrome Web Store. Para obtener más información, consulte Instalación desde Chrome Web Store.

Tras la instalación, la aplicación Citrix Workspace debe configurarse con los datos de conexión de Citrix Gateway y del sitio de Citrix Receiver para Web que proporciona los escritorios y las aplicaciones de los usuarios. Esta configuración puede hacerse de dos maneras:

- Puede generar un archivo **CR** que contenga los datos de conexión adecuados y distribuir este archivo a los usuarios. Para configurar la aplicación Citrix Workspace para ChromeOS, los usuarios deben hacer doble clic en el archivo **CR** y hacer clic en Agregar cuando se les solicite. Para obtener más información acerca de la generación de archivos CR desde StoreFront, consulte Exportar archivos de aprovisionamiento de almacenes para los usuarios.
- Puede proporcionar a los usuarios la URL que deben introducir la primera vez que inicien la aplicación Citrix Workspace para ChromeOS.

Reempaquetado

Para simplificar el proceso de implementación para los usuarios, puede reempaquetar la aplicación Citrix Workspace para ChromeOS con un nuevo archivo **CR** y preconfigurar la aplicación Citrix Workspace para ChromeOS con los datos de conexión adecuados de su entorno. Los usuarios pueden comenzar a trabajar con la aplicación Citrix Workspace para ChromeOS cuando la hayan instalado, no necesitan seguir más pasos de configuración.

1. Descargue la versión sin empaquetar de la aplicación Citrix Workspace para ChromeOS a una ubicación adecuada.
2. Descargue el archivo de configuración de ejemplo y modifíquelo para adaptarlo a su entorno.
3. Cambie el nombre del archivo de configuración modificado a default.cr y cópielo en el directorio raíz de la aplicación Citrix Workspace para ChromeOS.

   Los archivos de configuración con nombres distintos o situados en otras ubicaciones no se incluirán cuando la aplicación Citrix Workspace para ChromeOS se reempaquete.

4. De forma predeterminada, está habilitada la barra de herramientas de la sesión. Si quiere inhabilitar la barra de herramientas de la sesión, siga estos pasos.

   Nota: Le recomendamos que haga una copia de seguridad del archivo configuration.js antes de modificarlo.

   a) Utilice un editor de texto para abrir el archivo configuration.js en el directorio raíz de la aplicación Citrix Workspace para Chrome.

   b) Busque la siguiente sección en el archivo.

   ```
   pre codeblock 'appPrefs':{ 'chromeApp':{ 'ui': { 'toolbar': {
    'menubar':true, 'clipboard': false <!--NeedCopy-->
   ```

   c) Cambie el parámetro del atributo "menubar"a **false**.

   Nota: Para anular cualquier configuración anterior, le recomendamos que utilice la consola de administración de Google para enviar la directiva.

5. De forma predeterminada, la aplicación Citrix Workspace para ChromeOS puede abrir cualquier extensión de archivo mediante la aplicación Archivos de Chromebook. Puede usar el Chromebook destinado a abrir archivos en Google Drive con el componente FileAccess del VDA.

   Si un administrador quiere inhabilitar esta opción para descargar la versión no empaquetada de la aplicación Citrix Workspace y modificar la sección de "file handlers"en manifest.json para que se asemeje a lo siguiente:

   ```
   "file handlers" : {

           "text" :
               "extensions" :  [
                    "ica",
                     "cr"
                ]
              }

       }

   <!--NeedCopy-->
   ```

6. En Chrome, vaya a chrome://extensions, marque la casilla **Modo de desarrollador** de la esquina superior derecha de la página y, a continuación, haga clic en el botón **Empaquetar extensión**.

   Por motivos de seguridad, StoreFront solo acepta conexiones de instancias conocidas de la aplicación Citrix Workspace para ChromeOS. Debe agregar su aplicación reempaquetada a la lista de permitidos para que los usuarios puedan conectarse a un sitio de Citrix Receiver para Web.

7. En el servidor de StoreFront, utilice un editor de texto para abrir el archivo web.config del sitio de Citrix Receiver para Web, que se encuentra en el directorio web **C:\inetpub\wwwroot\Citrix\storename**. El *storename* es el nombre especificado para el almacén cuando este se creó.

8. Localice los siguientes elementos en el archivo.

   ```
   pre codeblock <html5 ... chromeAppOrigins="chrome-extension://
   haiffjcadagjlijoggckpgfnoeiflnem"... /> <!--NeedCopy-->
   ```

9. Cambie el valor del atributo **chromeAppOrigins** a chrome-extension:*//ID del paquete*, donde **ID del paquete** es el ID generado por la aplicación reempaquetada.

Compilaciones de reserva y de acceso anticipado

Existe la opción de usar compilaciones de reserva y de acceso anticipado de la aplicación Citrix Workspace para ChromeOS. La compilación de reserva proporciona continuidad de negocio si hay algún problema en curso en la compilación de producción. Antes de continuar, familiarícese con estos ID de compilación:

- `haiffjcadagjlijoggckpgfnoeiflnem`: Es el ID de la versión publicada de la aplicación Citrix Workspace para ChromeOS en Chrome Web Store.
- `lbfgjakkeeccemhonnolnmglmfmccaag`: Es el ID de la versión de acceso anticipado (EAR) de la aplicación Citrix Workspace para ChromeOS.
- `anjihnbmjbbpofafpmklejenkgnjfcdi`: Es el ID de la compilación de reserva de la aplicación Citrix Workspace para ChromeOS. La compilación de reserva tiene el contenido de la versión anterior a la versión de producción actual con un ID de versión diferente.

Para acceder a la compilación de reserva

Para acceder a la compilación de reserva, haga esto:

1. Haga clic en el enlace https://chrome.google.com/webstore/detail/citrix-workspace-backup/anjihnbmjbbpofafpmklejenkgnjfcdi.

   Se muestra la página de la extensión Backup de la aplicación Citrix Workspace.

2. Haga clic en **Agregar a Chrome**.

   La aplicación se instala. Vaya a `chrome://extensions` en su explorador web Chrome para ver la extensión.

3. Busque la aplicación Citrix Workspace en ChromeOS Launcher para usarla.

Para acceder a la compilación de EAR

Para acceder a la versión EAR, haga lo siguiente:

1. Haga clic en el enlace https://chrome.google.com/webstore/detail/citrix-workspace-backup/lbfgjakkeeccemhonnolnmglmfmccaag.

   Aparece la página de la extensión de la aplicación Citrix Workspace para Chrome S.

2. Haga clic en **Agregar a Chrome**.

   La aplicación se instala. Vaya a `chrome://extensions` en su explorador web Chrome para ver la extensión.

3. Busque la aplicación Citrix Workspace en ChromeOS Launcher para usarla.

Compatibilidad con ChromeOS LTS

Google tiene la versión de asistencia a largo plazo (LTS) en ChromeOS si prefiere menos actualizaciones. En cualquier momento, una o más versiones de la aplicación Citrix Workspace son compatibles con la versión más reciente de ChromeOS LTS.

Si busca una versión de la aplicación Citrix Workspace con las correcciones de errores y funciones más recientes, le recomendamos:

- Usar la versión más reciente de la aplicación Citrix Workspace
- Usar la versión más reciente de Google ChromeOS en el canal estable.

Compatibilidad con versiones anteriores

Es posible que las correcciones de errores en la aplicación Citrix Workspace o ChromeOS no sean compatibles con versiones anteriores de ChromeOS LTS. Para acceder a la compatibilidad con versiones anteriores, es posible que deba cambiar al canal estable de ChromeOS.

Es posible que las nuevas funciones que ofrecen Citrix o Google dependan de versiones de software más recientes. Para acceder a nuevas funciones, utilice el canal estable de ChromeOS y la versión más reciente de la aplicación Citrix Workspace.

Exclusiones

Estas funciones no cumplen los requisitos de compatibilidad con ChromeOS LTS:

- Optimización de Microsoft Teams
- Redirección de contenido del explorador web

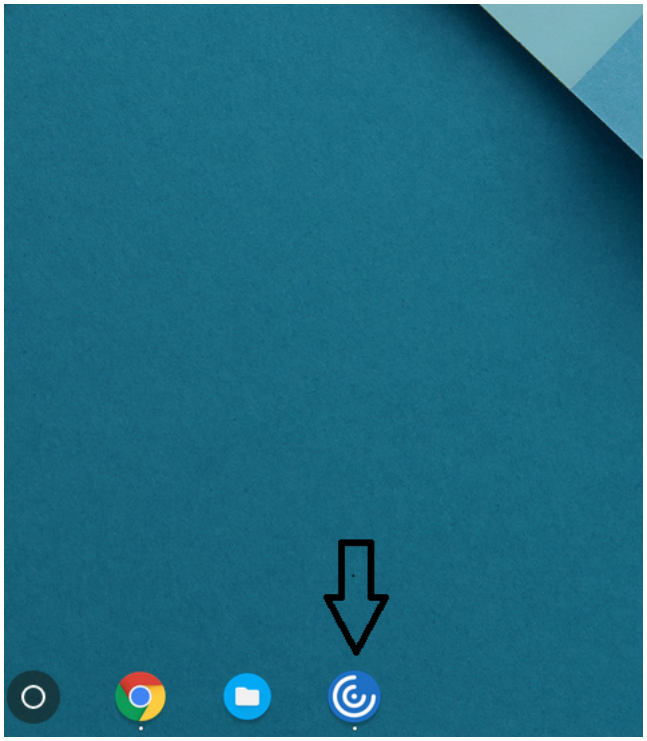
Hay actualizaciones de las funciones excluidas disponibles en la versión más reciente de ChromeOS en el canal estable, junto con la versión más reciente de la aplicación Citrix Workspace.

Preguntas frecuentes

- ¿Cómo sé qué versión de la aplicación Citrix Workspace es compatible con la versión más reciente de ChromeOS LTS?
  - Encontrará la versión más reciente en la página Acerca de esta versión.
  - Puede encontrar el archivo instalable de la versión más reciente en la página Descargas de Citrix.
- Como administrador, ¿cómo puedo realizar pruebas en el canal de ChromeOS LTS?
  - Para obtener más información, consulta Long-term support releases en la página educativa de Google ChromeOS.
- Como administrador, ¿qué debo hacer si tengo algún problema al utilizar ChromeOS LTS con la aplicación Citrix Workspace?
  - Compruebe si observa el mismo problema con la versión más reciente de ChromeOS en el canal estable junto con la versión más reciente de la aplicación Citrix Workspace. En caso afirmativo, notifique el problema a través de sus canales de asistencia habituales. De lo contrario, actualice la versión a aquella en la que no vio el problema.

Desinstalar

Después de instalar y configurar la aplicación Citrix Workspace, seleccione el icono de Citrix Workspace en la lista de aplicaciones de Chrome. La aplicación Citrix Workspace para ChromeOS se inicia como se muestra en esta imagen. Para quitar la aplicación Citrix Workspace para ChromeOS de los dispositivos, debe hacer clic con el botón secundario en el icono de la aplicación Citrix Workspace, en la lista de aplicaciones de Chrome, y seleccionar **Desinstalar**.



Actualizaciones

Para actualizar la versión de la aplicación que tenga a la nueva aplicación Citrix Workspace, siga uno de estos pasos:

- Descargue la aplicación Citrix Workspace de la página de descargas de Citrix e instale la aplicación para actualizar la aplicación Citrix Receiver a la aplicación Citrix Workspace.
- Actualice su aplicación Citrix Workspace mediante el almacén de aplicaciones del sistema operativo.
- En Windows y macOS, actualice automáticamente a la aplicación Citrix Workspace desde Citrix Receiver mediante Actualizaciones de Citrix Receiver.

Para obtener la documentación de Citrix Receiver para Chrome, consulte Citrix Receiver.

Introducción

May 16, 2024

Configuración

Las aplicaciones y los escritorios aparecen después de iniciar sesión. Puede buscar recursos y hacer clic en cualquier icono para iniciar un escritorio o una aplicación en una ventana nueva.

Cuando se inicia una aplicación más, la aplicación Citrix Workspace para ChromeOS comprueba si esta se puede iniciar en una sesión existente antes de crear otra sesión. Esta función le permite acceder a muchas aplicaciones en una sola sesión.

Puede configurar las funcionalidades y las características de la aplicación Citrix Workspace para ChromeOS mediante uno de los siguientes métodos:

- Directiva administrativa de Google
- Web.config en StoreFront
- default.ica
- configuration.js

> **Nota:**
>
> Con la versión 1901, la pantalla de presentación ya no es visible para los usuarios. El esquema **"splashScreen": false** ya no se admitirá en futuras versiones. Debe eliminar el esquema, si está presente, de la directiva de administración de Google o del archivo configuration.js.

Mediante la directiva de administración de Google

> **Nota:**
>
> Citrix recomienda usar este método solo cuando se reempaquete la aplicación Citrix Workspace para ChromeOS para los usuarios.

Antes de la versión 2.1, solo se podían enviar configuraciones relacionadas con almacenes o balizas mediante la directiva de administración de Google (Google Admin Policy). Para ver información adicional sobre esta directiva, consulte los artículos CTX141844 y CTX229141 de Knowledge Center.

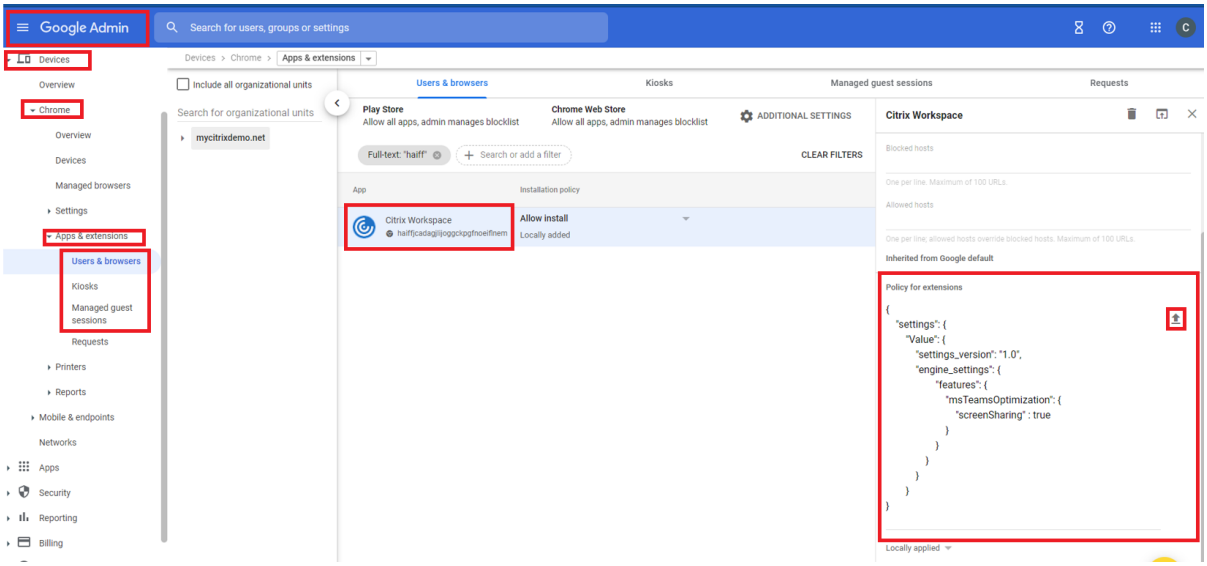
Con la versión 2.1 de la aplicación Citrix Workspace para ChromeOS, otras configuraciones de Chrome también pueden enviarse a través de la directiva de administración de Google.

Cómo enviar directivas a través de la consola de administración de Google

Para enviar directivas a través de la consola de administración de Google, siga estos pasos:

1. En la **consola de administración de Google**, seleccione **Devices > Chrome > Apps & extensions > Users & browsers**.

2. Busque la aplicación Citrix Workspace (introduzca el ID de aplicación del almacén web; por ejemplo, `haiffjcadagjlijoggckpgfnoeiflnem`).
3. Haga clic en el icono de la aplicación Citrix Workspace.
4. Aparece la directiva de extensiones. Copie y pegue la directiva o cargue el archivo policy.txt con el JSON correspondiente.
5. Haga clic en **Guardar**.
6. Repita los pasos para **Kiosk** y **Managed guest sessions** si es necesario.



Para obtener más información, consulte la asistencia técnica de Google.

Verificar la configuración de directivas

Para comprobar que las directivas se envían correctamente, lleve a cabo los siguientes pasos:

1. Vaya a `chrome://policy/`.
2. Haga clic en `Reload policies`.
3. Busque el ID de Chrome Web Store de la aplicación Citrix Workspace para ChromeOS, que es `haiffjcadagjlijoggckpgfnoeiflnem`.
    - Si las directivas se envían correctamente desde la consola de administración de Google, aparecerán en el ID del almacén web: `haiffjcadagjlijoggckpgfnoeiflnem`. De lo contrario, compruebe que las directivas estén configuradas correctamente. Para crear o modificar la directiva, debe utilizar `Configuration Utility Tool`.
    - Si las directivas aparecen en el ID del almacén web, pero no surten efecto en la sesión, contacte con la asistencia técnica de Citrix.

Mediante web.config

> **Nota:**
>
> Citrix recomienda usar el método del archivo **web.config** para la configuración solo cuando se esté usando una versión de la tienda de aplicaciones de la aplicación Citrix Workspace para ChromeOS.

Para cambiar la configuración mediante el método del archivo web.config (solo para aquellos que usan instancias locales de StoreFront):

1. Abra el archivo **web.config** del sitio de Citrix Receiver para Web. Este archivo se encuentra en **C:\inetpub\wwwroot\Citrix\<storenameWeb>**, donde *storename* es el nombre especificado para el almacén cuando se creó.
2. Busque el campo **chromeAppPreferences** y defina su valor con la configuración como cadena JSON.

Por ejemplo:

```
chromeAppPreferences = {

    "ui": {

        "toolbar": {

            "menubar": false
             }

             }

             }

<!--NeedCopy-->
```

Aquí tiene otro ejemplo:

Mediante default.ica

> **Nota:**
>
> Citrix recomienda usar el método del archivo **default.ica** con fines de configuración solo para usuarios de la Interfaz Web.

La aplicación Citrix Workspace para ChromeOS permite archivos ICA personalizados sin ningún valor de programa inicial.

Para cambiar la configuración mediante el archivo **default.ica**:

1. Abra el archivo default.ica en **C:\inetpub\wwwroot\Citrix\<nombre del sitio>\conf\default.ica** para los clientes de la Interfaz Web, donde **nombre del sitio** es el nombre especificado para el sitio cuando se creó.
   Para los clientes de StoreFront, el archivo **default.ica** se encuentra en **C:inetpubwwwrootCitrix\<Storenam** donde **Storename** es el nombre que se especificó para el almacén cuando se creó.
2. Agregue una clave al final del archivo, **chromeAppPreferences**, con el valor definido con la configuración como objeto JSON.

Por ejemplo:

```
chromeAppPreferences={

    "ui":{

        "toolbar": {

```



```
            "menubar": false
             }

             }

             }

<!--NeedCopy-->
```

Este es el aspecto de un archivo **default.ica** de ejemplo:

web.config | default.ica

```
[Application]
TransportDriver=TCP/IP
DoNotUseDefaultCSL=On
BrowserProtocol=HTTPonTCP
LocHttpBrowserAddress=!
WinStationDriver=ICA 3.0
ProxyTimeout=30000
AutologonAllowed=ON
TWIMode=Off
FontSmoothingType=0

[EncRC5-0]
DriverNameWin16=pdc0w.dll
DriverNameWin32=pdc0n.dll

[EncRC5-40]
DriverNameWin16=pdc40w.dll
DriverNameWin32=pdc40n.dll

[EncRC5-56]
DriverNameWin16=pdc56w.dll
DriverNameWin32=pdc56n.dll

[EncRC5-128]
DriverNameWin16=pdc128w.dll
DriverNameWin32=pdc128n.dll

[Compress]
DriverNameWin16=pdcompw.dll
DriverNameWin32=pdcompn.dll

chromeAppPreferences = '{"ui":{"toolbar":{"menubar":false,"displayResolution":false}}}'
```

Mediante el archivo configuration.js

El archivo **configuration.js** se encuentra en la **carpeta raíz de ChromeApp**. Acceda a este archivo directamente para modificar la aplicación Citrix Workspace para ChromeOS.

> **Nota:**
>
> - Citrix recomienda hacer una copia de seguridad del archivo configuration.js antes de modificarlo.
> - Se necesitan credenciales de nivel de administrador para modificar el archivo configura-

> tion.js file. Después de modificarlo, reempaquete la aplicación para hacer otras modificaciones en los elementos de la barra de herramientas.
> - En modo quiosco, la barra de herramientas está oculta de forma predeterminada. Cuando modifique el archivo configuration.js para habilitar la barra de herramientas, verifique que el modo quiosco está inhabilitado. Citrix recomienda usar uno de los métodos alternativos (por ejemplo, el archivo default.ica) para habilitar la barra de herramientas.

Marca personalizada de logotipos e iconos

Puede personalizar como quiera el logotipo y los iconos de la aplicación Citrix Workspace para aplicaciones y escritorios. Puede personalizarlos de esta manera:

1. Instale la aplicación Citrix Workspace para ChromeOS desde Chrome Web Store.
2. Vaya a la carpeta **/chromeAppUI/resources/images**.
3. Sustituya estas imágenes por las imágenes que quiera, pero con las mismas dimensiones:
    - icon_16x16.png
    - icon_32x32.png
    - icon_48x48.png
    - icon_128x128.png
    - icon_256x256.png
4. Vaya a la **carpeta raíz de ChromeApp** y abra el archivo **manifest.json**.
5. Sustituya el valor del nombre y la descripción por el texto requerido.
6. Guarde los cambios.
7. Cargue de nuevo la aplicación desde la página Extensiones.

Configurar

May 16, 2024

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.

Modo de configuración

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 directiva.

Puede habilitar el tráfico y la comunicación en LaunchDarkly de las siguientes formas:

Permitir el tráfico a las siguientes URL

- events.launchdarkly.com
- app.launchdarkly.com

Incluir direcciones IP en una lista de permitidos Si necesita incluir las direcciones IP en una lista de permitidos, para obtener una lista de todos los intervalos de direcciones IP actuales, consulte esta lista de direcciones IP públicas de LaunchDarkly. Puede usar esta lista para verificar que las configuraciones de su firewall se actualicen automáticamente de acuerdo con las actualizaciones de la infraestructura. Para obtener detalles sobre el estado actual de los cambios en la infraestructura, consulte la Página de estado de LaunchDarkly.

Disposición para inhabilitar el servicio de LaunchDarkly Puede inhabilitar el servicio de LaunchDarkly tanto en almacenes locales como de la nube.

En la configuración de la nube, los administradores pueden inhabilitar el servicio de LaunchDarkly al establecer el atributo **enableLaunchDarkly** en **False** en Global App Configuration Service.

Para obtener más información, consulte la documentación de Global App Configuration Service.

En la implementación local, los administradores pueden inhabilitar el servicio de LaunchDarkly mediante la directiva administrativa de Google de esta manera:

1. Inicie sesión en la Consola de administración de Google.
2. Vaya a **Administración de dispositivos** > **Administración de Chrome** > **Configuración de usuario**.
3. Agregue estas cadenas al archivo **policy.txt** en la clave **engine_settings**.

```
"thirdPartyServices": {


  "enableLaunchDarkly": false

 }
 ,
```



```
8
9  <!--NeedCopy-->
```

4. Haga clic en **Guardar**.

> **Nota:**
>
> - De forma predeterminada, el servicio LaunchDarkly está habilitado si el atributo **enableLaunchDarkly** no está presente.

En la implementación local, los administradores pueden inhabilitar el servicio de LaunchDarkly mediante el archivo configuration.js de esta manera:

> **Nota:**
>
> - Se necesitan credenciales de nivel de administrador para modificar el archivo configuration.js. Después de modificarlo, vuelva a empaquetar la aplicación para que las modificaciones surtan efecto.

1. Abra el archivo **configuration.js**.
2. Agregue el atributo **enableLaunchDarkly** y defina el atributo en **false**.

```
1  "thirdPartyServices": {
2
3
4      "enableLaunchDarkly": false
5
6        }
7   ,
8  <!--NeedCopy-->
```

3. Haga clic en **Guardar**.

> **Nota:**
>
> - De forma predeterminada, el servicio LaunchDarkly está habilitado si el atributo **enableLaunchDarkly** no está presente.

Nota sobre el JSON de configuración

Con la versión 2202.1 (22.2.1.8), la aplicación Citrix Workspace solo acepta JSON válidos para enviar la configuración. Haga lo siguiente para validar el archivo JSON:

1. Verifique los datos de JSON. Use el enlace https://jsonlint.com/ para verificarlo.
2. Siga los pasos mencionados en la página Introducción para actualizar:
    - Directiva de Google

- web.config
- default.ica
- configuration.js

Se recomienda utilizar la herramienta de utilidad de configuración para generar parámetros JSON válidos para personalizar la aplicación Citrix Workspace para ChromeOS mediante:

- configuration.js
- web.config
- default.ica
- Directiva de Google

> **Nota**:
>
> Es posible que tenga problemas al iniciar sesión cuando el JSON de configuración no es válido.

Parámetro de proxy HTTP en Chromebook

Si ha configurado el parámetro del proxy HTTP en su Chromebook, es posible que sus sesiones no se inicien.

Para resolver este problema, puede inhabilitar el parámetro **nativeSocket** en la consola de administración de Google y asegurarse de que ha habilitado la directiva **Conexiones de WebSockets** en DDC. Para obtener más información, consulte el artículo WebSocket.

A continuación se muestra un ejemplo de datos JSON:

```
{

        "settings": {

        "Value": {

              "settings_version": "1.0",
              "engine_settings": {

                          "transport":
                                 {
  "nativeSocket": false
                                     }

                               }

                        }

           }

 }

```



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

> **Advertencia:**
>
> Al deshabilitar el atributo **nativeSocket** se habilita la conexión de WebSocket, lo que puede afectar al rendimiento en comparación con el uso de un socket nativo.

Modo quiosco

El modo quiosco de la aplicación Citrix Workspace para ChromeOS le ayuda a ejecutar todas las aplicaciones en la misma ventana. Con esta funcionalidad, se pueden ejecutar aplicaciones de Citrix Workspace en modo quiosco y luego iniciar cualquier escritorio o aplicación de Windows mediante el mismo modo. Además, el modo quiosco permite publicar aplicaciones o escritorios remotos como paquetes Chrome dedicados mediante una URL persistente.

Modo de configuración

Para controlar esta función, puede ajustar los parámetros de quiosco en el panel de administración de Chrome. Este parámetro solo se aplica a dispositivos Chrome administrados.

Consulte el sitio de asistencia de Google para obtener instrucciones sobre cómo habilitar la aplicación Citrix Workspace para ejecutarse en modo quiosco en dispositivos Chrome administrados y no administrados.

Si piensa implementar una aplicación Citrix Workspace, debe publicar mediante las opciones de visibilidad configuradas como `Public/unlisted` para verificar la interoperabilidad con el modo quiosco. Vaya al Panel para desarrolladores de Chrome Web Store

La URL del almacén es de solo lectura cuando el modo quiosco está activo y no se puede modificar desde la pantalla de parámetros de **Cuenta**. Sin embargo, puede cambiar este parámetro de una de las siguientes maneras:

- Reempaquetar la aplicación con el archivo `.cr`.
- Mediante la consola de administración de Google. Use la gestión de políticas de Google para acceder a la consola de administración de Google.

```
    <Services version="1.0">
    <Service>
    <rfWeb>http://your_RfWebURL_or_persistenturl</rfWeb>
    <Name>Mystore</Name>
    <Gateways>
    <Gateway>
    <Location>https://yourcompany.gateway.com</Location>
    </Gateway>
    </Gateways>
```



```
    <Beacons>
    <Internal>
    <Beacon>http://yourcompany.internalwebsite.net</Beacon>
    </Internal>
    <External>
    <Beacon>http://www.yourcompany.externalwebsite.com</Beacon>
    </External>
    </Beacons>
    </Service>
    </Services>

<!--NeedCopy-->
```

Si usa la consola de administración de Google, modifique el archivo **policy.txt** que contiene la configuración de Citrix Workspace. Sustituya el valor de "url"bajo "rf_web"por una URL persistente.

```
    {

    "settings": {

    "Value": {

    "settings_version": "1.0",
    "store_settings": {

    "beacons": {

    "external": [
    {

    "url": "http://www.yourcompany.externalwebsite.com"
     }

    ],
    "internal": [
    {

    "url": "http://yourcompany.internalwebsite.net"
     }

    ]
     }
 ,
    "gateways": [
    {

    "is_default": true,
    "url": "https://yourcompany.gateway.com"
     }

    ],
    "name": "mystore",
    "rf_web": {
```



```
38
39      "url": " http://your_RfWebURL_or_persistenturl "
40       }
41
42       }
43
44       }
45
46       }
47
48       }
49
50  <!--NeedCopy-->
```

Global App Configuration Service

A partir de esta versión, como administrador, puede usar Global App Configuration Service para:

- administrar y configurar de forma centralizada los parámetros de la aplicación y establecer valores predeterminados;
- aplicar la configuración en dispositivos administrados y no administrados (BYOD);
- aplicar la configuración tanto para los usuarios de la nube (dominio reclamado) como para los usuarios locales (URL reclamada).

Para obtener más información, consulte la documentación de Global App Configuration Service.

> **Notas:**
>
> Esta función solo está disponible para almacenes de espacio de trabajo y HTTPS.
> Para que Global App Configuration Service funcione, verifique que sus usuarios puedan acceder a las direcciones URL `https://discovery.cem.cloud.us`, `https://gacs-discovery.cloud.com` y `https://gacs-config.cloud.com`.

Programa para la mejora de la experiencia del usuario (CEIP)

May 16, 2024

Modo de configuración

Datos recopilados	Descripción	Para qué se usan
Datos de uso y configuración	El programa para la mejora de la experiencia del usuario de Citrix (Customer Experience Improvement Program o CEIP) recopila información de uso y configuración de la aplicación Citrix Workspace y envía esos datos automáticamente a Citrix y a Google Analytics.	Esos datos ayudan a Citrix a mejorar la calidad, la fiabilidad y el rendimiento de la aplicación Citrix Workspace.

Información adicional

Citrix gestiona sus datos de acuerdo con las condiciones de su contrato. Citrix protege sus datos como se especifica en Citrix Services Security Exhibit, disponible en el Centro de confianza de Citrix.

Citrix utiliza Google Analytics para recopilar determinados datos de la aplicación Citrix Workspace como parte del programa CEIP. Puede inhabilitar o bloquear los datos de CEIP. Revise cómo gestiona Google los datos recopilados para Google Analytics.

> **Nota:**
>
> No se recopilan datos de los usuarios de la Unión Europea (UE) ni del Espacio Económico Europeo (EEE) ni de Suiza ni del Reino Unido.

Datos de CEIP a Citrix y Google Analytics

A partir de la versión 2203, los usuarios finales pueden:

- decidir si quieren enviar los datos de uso a Citrix y Google Analytics o no
- bloquear CEIP a través de la GUI

Inhabilitación de CEIP

Puede inhabilitar el envío de datos de CEIP a Citrix y a Google Analytics. Para ello, utilice uno de los métodos siguientes:

- Inhabilite CEIP mediante la directiva de administración de Google
- Inhabilite CEIP mediante el archivo configuration.js

> **Nota:**
>
> Al inhabilitar CEIP para la versión 2203 y versiones posteriores, se carga información mínima sobre la versión de la aplicación Citrix Workspace que está instalada. Esta información mínima es valiosa para Citrix porque le permite conocer la distribución de las distintas versiones utilizadas por los clientes.

Para inhabilitar CEIP mediante la directiva de administración de Google

> **Nota:**
>
> Se necesitan credenciales de nivel de administrador para realizar este procedimiento.

1. Inicie una sesión en la Consola de administración de Google.
2. Vaya a **Administración de dispositivos > Administración de Chrome > Configuración de usuario**.
3. Agregue las cadenas que se muestran después del paso 4 al archivo policy.txt bajo la clave **engine_settings**.
4. Haga clic en **Guardar**.

Para obtener más información sobre la directiva de Google, consulte el artículo CTX141844 de Knowledge Center.

Para las versiones 1907 y anteriores, establezca el atributo enabled de **ceip** en **false**.

```
"ceip":{

    "enabled":false,
 }

<!--NeedCopy-->
```

Para las versiones 1908 y posteriores, establezca el atributo enabled de **analytics** en **false**. Sin embargo, la clave **analytics** es compatible con la clave **ceip** de versiones anteriores.

```
"analytics":{

    "enabled":false,
 }

<!--NeedCopy-->
```

Para inhabilitar CEIP mediante configuration.js

El archivo **configuration.js** se encuentra en la **carpeta raíz de ChromeApp**. Modifique este archivo para configurar la aplicación Citrix Workspace para ChromeOS.


```
> **Notes:**
>
> -  Citrix recommends that you back up the **configuration.js** file before making changes.
> -  Citrix recommends editing the **configuration.js** file, only if the Citrix Workspace app for ChromeOS is repackaged for users.
> -  Administrator-level credentials are required to edit the **configuration.js** file.
```

Para las versiones 1907 y anteriores, establezca el atributo enabled de **ceip** como **false** en el archivo **configuration.js**.

```
"ceip":{

    "enabled":false,
 }

<!--NeedCopy-->
```

Para las versiones 1908 y posteriores, establezca el atributo enabled de **analytics** como **false** en el archivo **configuration.js**.

```
"analytics":{

    "enabled":false,
 }


<!--NeedCopy-->
```

Bloqueo de CEIP

Para las versiones 2007 y posteriores, los administradores pueden bloquear CEIP a través del archivo configuration.js y de la directiva de administración de Google.

Para la versión 2203 y posteriores, los usuarios finales pueden bloquear CEIP a través de la GUI.

Esta configuración tiene prioridad sobre la establecida a través de la GUI y la directiva de administración de Google, y los datos de CEIP no se envían a Citrix.

Para bloquear CEIP mediante la directiva de administración de Google

> **Nota:**
>
> Se necesitan credenciales de nivel de administrador para realizar este procedimiento.

1. Inicie una sesión en la Consola de administración de Google.

2. Vaya a **Administración de dispositivos > Administración de Chrome > Configuración de usuario**.
3. Agregue las cadenas que se muestran después del paso 4 al archivo policy.txt bajo la clave **engine_settings**.
4. Haga clic en **Guardar**.

```
"analytics":{

    "connectionEnabled":false,
                  }

<!--NeedCopy-->
```

Para bloquear CEIP mediante configuration.js

1. Abra el archivo configuration.js.
2. Agregue el atributo **connectionEnabled** y establezca el atributo en **false**:

```
"analytics":{

"connectionEnabled":false,
              }


<!--NeedCopy-->
```

Para bloquear CEIP mediante la GUI

> **Nota:**
>
> Solo el usuario final puede modificar la configuración de CEIP mediante la interfaz gráfica de usuario.

1. Inicie la aplicación Citrix Workspace para ChromeOS.
2. Seleccione **Parámetros > General**.
3. Desactive la opción **Ayudar a mejorar Citrix Workspace enviando estadísticas de uso anónimas**.

Reinicie la aplicación Citrix Workspace para que los cambios surtan efecto.

Datos específicos de CEIP

Elementos concretos de datos CEIP recopilados por Google Analytics:

Versión de la aplicación Citrix Workspace	Modo de sesión (quiosco, público o general)	Tipo de sesión (escritorio o aplicación)	Información de XenDesktop (versiones de Delivery Controller y VDA)
Tipo de inicio (SDK, archivo ICA, FTA, Store, etc.)	Zona horaria de la sesión	Idioma de la sesión	Distribución del teclado del cliente
Tipo de socket de red (HTTPS o HTTP)	Uso de funciones (portapapeles, transferencia de archivos, conmutador de aplicaciones, impresión, USB, tarjeta inteligente, etc.)	Proporción de píxeles del dispositivo	Secure ICA (se usa o no)
ID de recurso de los Chromebooks empresariales inscritos	Tiempo de espera de reconexión (if!= 180)	Varios monitores	Global App Configuration Service

Portapapeles

May 16, 2024

Función para copiar clips de imagen

Con los accesos directos de teclado estándar, puede copiar y pegar clips de imagen entre el dispositivo local y las sesiones de escritorio y aplicación virtuales. Puede utilizar los accesos directos estándar del teclado para copiar y pegar contenido. Por ejemplo, puede usar aplicaciones como Microsoft Word, Microsoft Paint y Adobe Photoshop. Antes, esta funcionalidad solo estaba disponible para texto.

> **Nota:**
>
> - Debido a las restricciones de ancho de banda de la red, es posible que las sesiones dejen de responder al intentar copiar y pegar un clip de imagen que ocupe más de 2 MB.
> - Puede seleccionar y presionar Ctrl + C y Ctrl + V para copiar y pegar. También se puede usar

> la funcionalidad de clic con el botón secundario para copiar o pegar contenido.
> - Hemos probado esta función con formatos BMP, PNG, JPEG y GIF.

Configuración del portapapeles

Puede copiar contenido HTML y conservar el formato cuando copia un enlace en Chrome. Se agrega una etiqueta <img> en formato HTML, lo que permite copiar imágenes y texto. Esta funcionalidad es más rica que el texto sin formato.

Para habilitar esta funcionalidad, agregue la siguiente entrada del Registro en el VDA:

HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Citrix\wfshell\Virtual Clipboard\Additional Formats\HTML Format
"**Name"="HTML Format**"

> **Advertencia**
>
> El uso incorrecto del Editor del Registro del sistema puede causar problemas graves que pueden hacer necesaria la reinstalación del sistema operativo. Citrix no puede garantizar que los problemas derivados de un uso incorrecto del Editor del Registro puedan resolverse. Si usa el Editor del Registro, será bajo su propia responsabilidad. Haga una copia de seguridad del Registro antes de modificarlo.

La función del portapapeles ha resuelto muchos problemas. Para obtener información adicional, consulte el artículo CTX086028 de Knowledge Center.

Formato de datos HTML

A partir de la versión 2207, puede usar el formato HTML en las operaciones del Portapapeles entre el escritorio virtual y el dispositivo de punto final. Al copiar y pegar los datos HTML, se copia el formato del contenido de origen. Al pegar los datos, el contenido de destino también incluye el formato. Además, el formato HTML proporciona un mejor diseño.

Para obtener más información sobre cómo configurar las directivas, consulte Formatos permitidos de escritura en el portapapeles del cliente en la documentación de Citrix Virtual Apps and Desktops.

El portapapeles admite el formato HTML

Puede usar el formato HTML en las operaciones del Portapapeles entre el escritorio virtual y el dispositivo de punto final. Al copiar los datos HTML, se copia el formato del contenido de origen y, al pegar los datos, el contenido de destino incluye el formato. Además, el formato HTML proporciona un mejor diseño.

Para obtener más información sobre cómo configurar las directivas, consulte Formatos permitidos de escritura en el portapapeles del cliente en la documentación de Citrix Virtual Apps and Desktops.

Procesamiento de archivos

May 16, 2024

Transferencia de archivos

La aplicación Citrix Workspace para ChromeOS proporciona una transferencia segura de archivos entre un dispositivo de usuario y una sesión. La sesión puede ser del tipo Citrix Virtual Apps and Desktops y Citrix DaaS Session. Esta función usa un canal virtual de transferencia de archivos en lugar de la asignación de unidades del cliente.

De manera predeterminada, los usuarios pueden:

- Cargar archivos desde una carpeta de descarga local o un periférico conectado
- Acceder de manera fluida a sus datos desde las sesiones de Citrix Virtual Apps and Desktops y Citrix DaaS.
- Descargue archivos de sus sesiones de Citrix Virtual Apps and Desktops y Citrix DaaS.
- Puede descargar archivos en una carpeta local o en un periférico del dispositivo del usuario.

Los administradores pueden configurar la transferencia de archivos, y la carga o descarga de archivos, mediante directivas en Citrix Studio.

> **Requisitos previos**

- XenApp o XenDesktop 7.6 o versiones posteriores, con:
  - Parche ICATS760WX64022.msp en los VDA de SO de servidor (Windows 2008 R2 o Windows 2012 R2)
  - Parche ICAWS760WX86022.msp o ICAWS760WX64022.msp en los VDA de SO de cliente (Windows 7 o Windows 8.1)
- Para cambiar las directivas de transferencia de archivos: Revisión hotfix de Administración de directivas de grupo (Group Policy Management) GPMx240WX64002.msi o GPMx240WX86002.msi en las máquinas que ejecutan Citrix Studio

> **Limitaciones de la función:**

- Los usuarios pueden cargar o descargar un máximo de 10 archivos a la vez.
- Tamaño máximo del archivo:

  - Para cargas: 2147483647 bytes (2 GB)
  - Para descargas: 262144000 bytes (250 MB)

- Si alguna de estas directivas, **Cargar archivos al escritorio** o **Descargar archivos desde el escritorio**, pero no ambas, están **inhabilitadas**, la barra de herramientas siempre muestra los iconos Cargar y Descargar. Sin embargo, la funcionalidad se basa en la configuración de la directiva. Si ambas directivas están **inhabilitadas**, los iconos de Cargar y Descargar no se muestran en la barra de herramientas.

Configurar directivas de transferencia de archivos

Para configurar la transferencia de archivos mediante una directiva de Citrix Studio

De forma predeterminada, la transferencia de archivos está habilitada.

Use Citrix Studio para cambiar estas directivas, ubicadas en **Configuración de usuario** > **ICA** > **Redirección de archivos**.

Directiva de Citrix Studio	Descripción
Permitir transferencia de archivos entre escritorio y cliente.	Para habilitar o inhabilitar la función de transferencia de archivos
Cargar archivos al escritorio.	Para habilitar o inhabilitar la carga de archivos dentro de la sesión. Requiere que la directiva "Permitir transferencia de archivos entre escritorio y cliente"esté configurada en true.
Descargar archivos desde el escritorio.	Para habilitar o inhabilitar la descarga de archivos desde la sesión. Requiere que la directiva "Permitir transferencia de archivos entre escritorio y cliente"esté configurada en true.

Para configurar la transferencia de archivos mediante el archivo configuration.js

El archivo **configuration.js** se encuentra en la **carpeta raíz de ChromeApp**. Modifique este archivo directamente para adaptar la aplicación Citrix Workspace a sus necesidades.

> **Notas:**
>
> - Citrix recomienda hacer una copia de seguridad del archivo **configuration.js** antes de hacer cambios.
> - Citrix recomienda modificar el archivo **configuration.js** solo si la aplicación Citrix Work-

space para ChromeOS se reempaqueta para los usuarios.
- Se requieren credenciales de nivel de administrador para modificar el archivo **configuration.js**. Tras modificar el archivo, reempaquete la aplicación para realizar más modificaciones en los elementos de la barra de herramientas.

Para cambiar la configuración de la barra de herramientas mediante el archivo configuration.js

Abra el archivo **configuration.js** y configure los parámetros como se indica a continuación:

Parámetros de cliente de transferencia de archivos	Descripción
AllowUpload	Para habilitar o inhabilitar la carga de archivos desde el lado del cliente. De forma predeterminada tiene el valor "true".
AllowDownload	Para habilitar o inhabilitar la descarga de archivos desde el lado del cliente. De forma predeterminada tiene el valor "true".
MaxUploadSize	Para establecer el tamaño máximo de los archivos que pueden cargarse, en bytes. De manera predeterminada, se ha establecido en 2 147 483 648 bytes (2 GB).
MaxDownloadSize	Para establecer el tamaño máximo de los archivos que pueden descargarse, en bytes. De manera predeterminada, se ha establecido en 2 147 483 648 bytes (2 GB).

A continuación se muestran los casos de funcionamiento cuando las directivas establecidas en Citrix Studio y el cliente son diferentes.

Directiva de Citrix Studio Carga / Descarga	Configuración en el cliente Carga / Descarga	Comportamiento resultante
INHABILITADO	HABILITADO	INHABILITADO
INHABILITADO	INHABILITADO	INHABILITADO
HABILITADO	INHABILITADO	INHABILITADO
HABILITADO	HABILITADO	HABILITADO

> **Nota:**
>
> Cuando se produce un conflicto entre el valor definido para el **tamaño máximo del archivo para cargar o descargar** en el Registro y el valor definido en los parámetros del lado del cliente, se aplicará el valor que indique un tamaño menor.

Para configurar la transferencia de archivos mediante la directiva administrativa de Google

De forma predeterminada, la función de transferencia de archivos está habilitada.

Para inhabilitarla, establezca el atributo enabled en false.

```
{

    "settings": {

        "Value": {

            "settings_version": "1.0",
                "engine_settings": {

                    "ui": {

                        "features": {

                           "filetransfer" : {

                                   "allowupload": true,
                                   "allowdownload": true,
                                   "maxuploadsize": 2147483647,
                                   "maxdownloadsize": 2147483647
                            }

                        }

                    }

                }

         }

     }

 }


<!--NeedCopy-->
```

Lista de opciones de transferencia de archivos, junto con sus descripciones:

- `allowupload`: Permite cargar archivos desde el dispositivo a la sesión remota.

- `allowdownload`: Permite descargar archivos del dispositivo a la sesión remota.
- `maxuploadsize`: Es el tamaño máximo de archivo, en bytes, que se puede cargar. De manera predeterminada, se ha establecido en 2 147 483 648 bytes (2 GB).
- `maxdownloadsize`: Es el tamaño máximo de archivo, en bytes, que se puede descargar. De manera predeterminada, se ha establecido en 2 147 483 648 bytes (2 GB).

Asignación de unidades del cliente

A partir de la versión 2307, la función de asignación de unidades del cliente (CDM) permite la asignación de carpetas en el dispositivo ChromeOS local, lo que permite acceder a ellas desde una sesión. Puede asignar carpetas del dispositivo ChromeOS, como, por ejemplo, carpetas de Descargas, Google Drive y unidades USB, si la carpeta no contiene archivos del sistema.

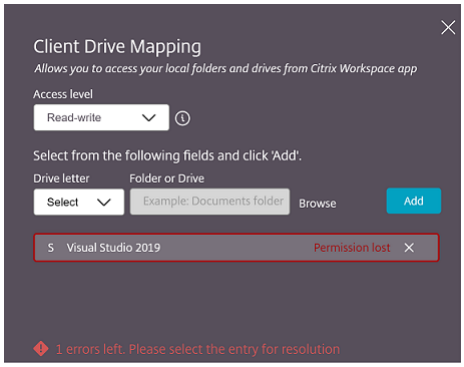
El usuario final puede realizar estas operaciones:

- Copie los archivos y las carpetas de la sesión a la unidad asignada y viceversa.
- Ver la lista de archivos y carpetas de la unidad asignada.
- Abra, lea y modifique el contenido de los archivos en la unidad asignada.
- Ver las propiedades de los archivos (solo la hora de la modificación y el tamaño de los archivos) en la unidad asignada.

Esta función ofrece la ventaja de acceder simultáneamente a unidades de escritorio virtuales y unidades de máquinas locales en el Explorador de archivos dentro de la sesión HDX.

Limitaciones conocidas

- No puede cambiar el nombre de archivos ni de carpetas dentro de la unidad asignada.
- Las asignaciones tienen el nombre de la carpeta, no la ruta completa.
- Si la carpeta local tiene archivos ocultos y ha asignado la misma carpeta, los archivos ocultos serán visibles dentro de la sesión en la unidad asignada.
- No puede cambiar la propiedad del archivo para que sea de solo lectura en la unidad asignada.
- CDM no está disponible cuando las sesiones se abren en modo incrustado con el SDK de HDX.
- Al asignar una carpeta de un dispositivo extraíble y quitar el dispositivo durante una sesión activa, no se puede usar la unidad asignada dentro de la sesión. Para quitar las asignaciones manualmente, haga clic en la marca **X** que hay al lado de la asignación en cuestión.



Configurar CDM

Puede configurar la función de CDM de una de estas maneras:

- Configuration.js
- Directiva administrativa de Google

> **Nota:**
>
> - Como requisito previo, un administrador debe habilitar la directiva **Redirección de unidades del cliente** en el Delivery Controller (DDC). Para obtener más información, consulte Redirección de unidades del cliente en la documentación de Citrix Virtual Apps and Desktops.

Configuration.js

Para inhabilitar la función CDM mediante el archivo **configuration.js**, haga lo siguiente:

1. Busque el archivo **configuration.js** en la carpeta **raíz de ChromeApp**.
2. Modifique el archivo para configurar la función de CDM.

   > **Notas:**
   >
   > - Citrix recomienda hacer una copia de seguridad del archivo **configuration.js** antes de hacer cambios.
   > - Citrix recomienda modificar el archivo **configuration.js** solo si la aplicación Citrix Workspace para ChromeOS se reempaqueta para los usuarios.
   > - Se requieren credenciales de nivel de administrador para modificar el archivo **configuration.js**.

3. Establezca el valor de **clientDriveMapping** en **false**.

   A continuación se muestra un ejemplo de datos JSON:


```
'features': {

    'clientDriveMapping': {

       'enabled': false,
       'availableAccessLevels': ["Read-write","Read-only,No-access
          "],
       'accessLevel': "Read-write"
     }

 }

<!--NeedCopy-->
```

4. Guarde los cambios.

Directiva administrativa de Google

Para los usuarios y dispositivos administrados, los administradores pueden inhabilitar la función de CDM mediante la directiva administrativa de Google de esta manera:

1. Inicie sesión en la directiva administrativa de Google.
2. Vaya a **Administración de dispositivos** > **Administración de Chrome** > **Configuración de usuario**.
3. Agregue estas cadenas al archivo **policy.txt**, en **engine_settings**.

   > **Nota:**
   >
   > También puede aplicar esta configuración en lo siguiente:
   >
   > - **Dispositivo** > **Chrome** > **Aplicaciones y extensiones** > **Quioscos** > Buscar la extensión > Política de extensiones.
   > - **Dispositivo** > **Chrome** > **Aplicaciones y extensiones** > **Sesiones de invitados gestionadas** > Buscar la extensión > Política de extensiones.

   A continuación se muestra un ejemplo de datos JSON:

```
{

"settings": {

    "Value": {

        "settings_version": "2.0",
        "engine_settings": {

            "features": {
```



```
11
12                  "clientDriveMapping": {
13
14                  "availableAccessLevels": ["Read-write", "Read-only
                       ","No-access"],
15                  "accessLevel": "Read-write"
16                                  }
17
18                          }
19
20                      }
21
22                   }
23
24               }
25
26   }
27
28 <!--NeedCopy-->
```

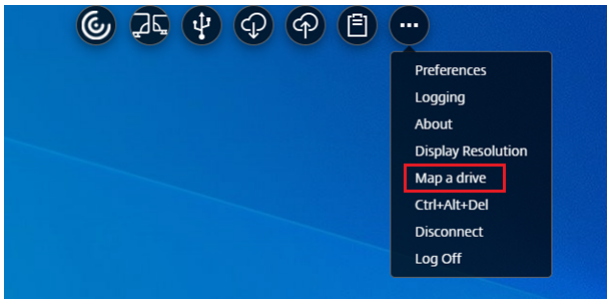
4. Guarde los cambios.

Nivel de acceso Puede configurar los niveles de acceso a la carpeta o a la unidad cuando la función está habilitada. Por ejemplo, si un administrador establece **availableAccessLevels** en [**"No-Access" , "Read-only"**], el usuario final puede ver las opciones **Read-Only Access** y **No-Access** en la lista desplegable.

Cómo utilizar la función CDM

En las sesiones de escritorio:

1. Vaya a la **Barra de herramientas** > **más (...)** > **Asignar una unidad**.

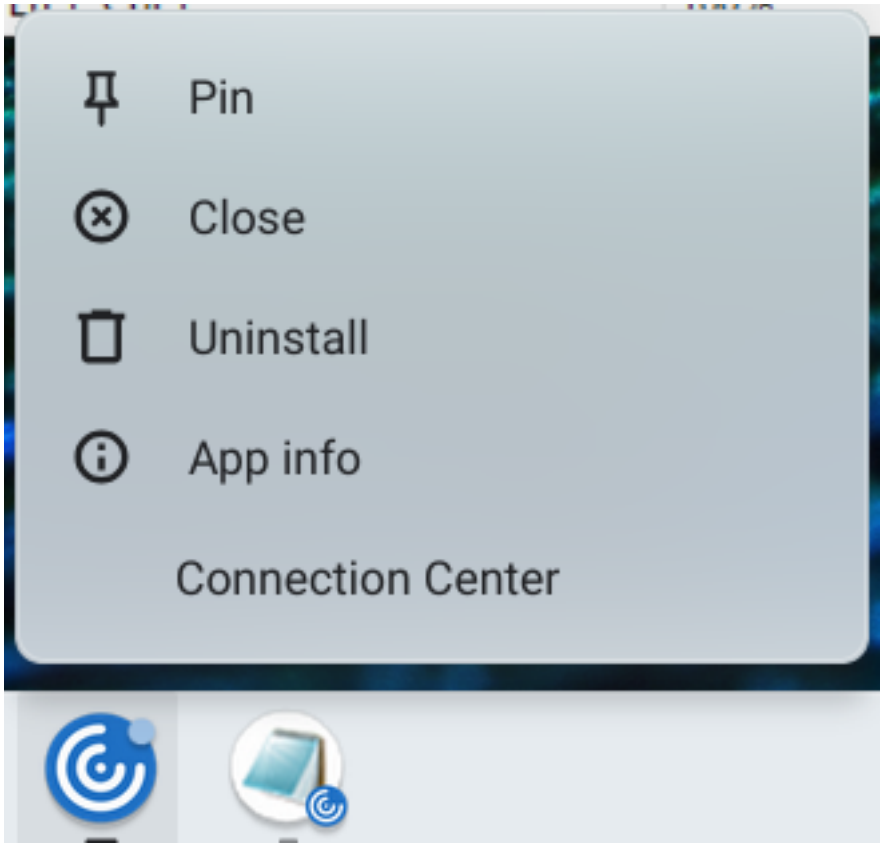


   Aparecerá el cuadro de diálogo de CDM.

2. Consulte la sección Cómo usar la interfaz de usuario de CDM para ver los pasos siguientes.

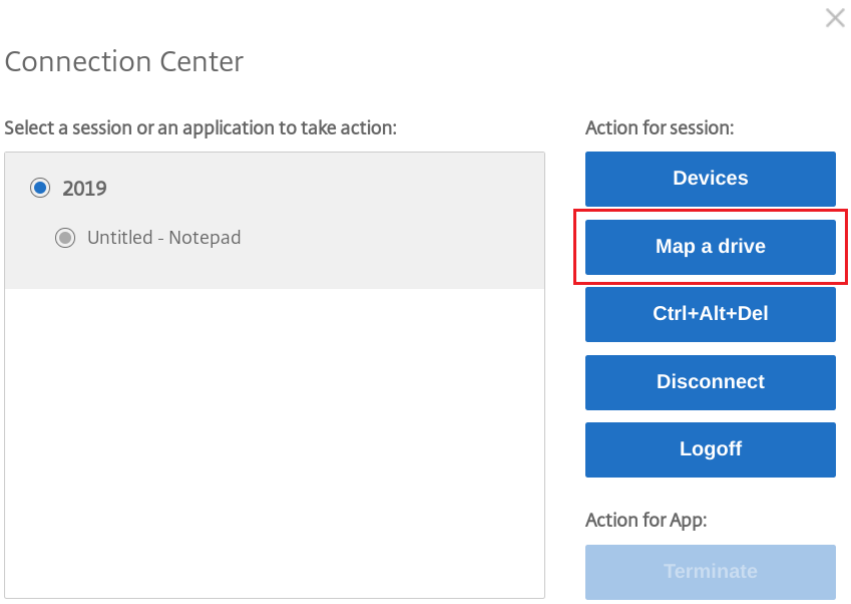
En las sesiones de aplicación y escritorio:

1. En la estantería de Chrome, haga clic con el botón secundario en el icono de la aplicación Citrix Workspace y seleccione **Central de conexiones**.



Aparece la pantalla **Central de conexiones**.

2. Seleccione la sesión y la aplicación. Haga clic en **Asignar una unidad**.

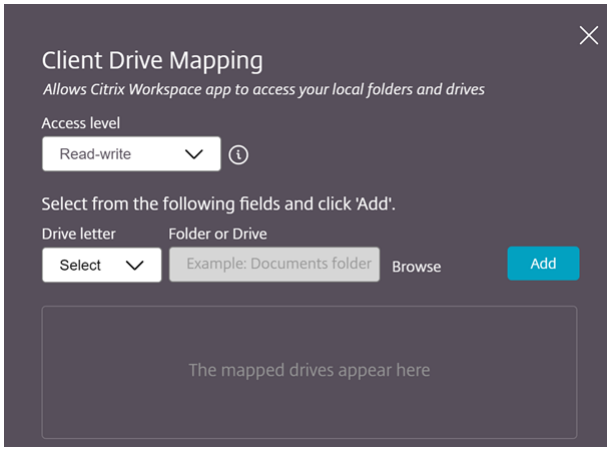


Aparecerá el cuadro de diálogo de CDM.

3. Consulte la sección Cómo usar la interfaz de usuario de CDM para ver los pasos siguientes.

Cómo usar la interfaz de usuario de CDM

1. Seleccione el **nivel de acceso** de la carpeta o la unidad. La opción de la lista desplegable que se muestra depende del nivel de acceso establecido por el administrador de TI de la organización para su perfil.



2. Seleccione una **letra de unidad** y haga clic en **Examinar** para ir a la carpeta o unidad en su Chromebook.
3. Haga clic en **Agregar**.
4. Desconecte y vuelva a conectar la sesión.

   Se mostrará la letra de unidad que está asignada dentro de la sesión.

Asociación de tipos de archivos

May 16, 2024

Acceso a Google Drive

Con la compatibilidad con Google Drive, los usuarios pueden abrir, modificar y guardar tipos de archivos de Windows desde un dispositivo Chrome que disponga de Citrix Workspace. Mientras están ejecutando un dispositivo Google Chrome, los usuarios pueden utilizar de forma fluida aplicaciones existentes basadas en Windows (por ejemplo, Microsoft Word) y acceder a los archivos que residen en Google Drive.

Si un usuario abre un archivo en Google Drive, lo modifica y lo guarda en Drive, se puede acceder al mismo archivo a través de la aplicación alojada de Citrix Virtual Apps. Por ejemplo, un archivo `.docx` adjunto descargado de Gmail. El archivo puede verse, modificarse y guardarse en Google Drive.

Modo de configuración

Requisitos previos

Para habilitar el acceso a Google Drive debe instalar el componente Citrix File Access (FileAccess.exe) en los VDA y habilitar la asociación de tipos de archivos en Citrix Studio. Citrix File Access se puede descargar desde la página de descargas de Citrix.

Para habilitar el acceso a Google Drive desde la aplicación Citrix Workspace

1. Instale `FileAccess.exe` en todas las instancias de Citrix Virtual Apps o el VDA de Citrix Virtual Apps and Desktops y Citrix DaaS.
2. En Citrix Studio, configure las asociaciones de tipos de archivos adecuadas para las aplicaciones publicadas.
3. Habilite las cookies y confíe en los sitios `https://accounts.google.com` y <`https://ssl.gstatic.com`>. Puede hacerlo en Citrix Virtual Apps o el VDA de Citrix Virtual Apps and Desktops y Citrix DaaS.

Solo se pueden abrir archivos de Google Drive mediante la aplicación Citrix Workspace. Para abrir un archivo desde Google Drive, haga clic con el botón secundario y abra el archivo mediante la aplicación Citrix Workspace.

Citrix recomienda asociar un tipo de archivo con una sola aplicación publicada.

Compatibilidad con configuración de proxy

La aplicación Citrix Workspace para ChromeOS permite abrir documentos desde Google Drive mediante aplicaciones publicadas a través de los servidores proxy no autenticados.

Modo de configuración:

Para habilitar la conexión de proxy, configure el parámetro de proxy en las opciones de Internet.

Para inhabilitar el acceso a Google Drive desde la aplicación Citrix Workspace

En el archivo manifest.json, reemplace:


```
"file_handlers" : {

      "all-file-types" : {

         "extensions" : [
            "*"
         ]
       }

    }
 ,
<!--NeedCopy-->
```

por:

```
    "file_handlers" : {

          "cr-file-type" : {

             "extensions" : [
                "cr",
               "ica"
             ]
           }

        }
 ,
<!--NeedCopy-->
```

Gráficos

June 18, 2024

Gráficos y H.264

Modo de configuración

Para configurar la compatibilidad con el protocolo H.264 y los gráficos, utilice la directiva de administración de Google para incluir lo siguiente. De forma predeterminada, la compatibilidad con el protocolo H.264 está habilitada. Para inhabilitarla, establezca el atributo enabled en false.

```
{

    "settings": {

```



```
        "Value": {

            "settings_version": "1.0",
                "engine_settings": {

                    "ui": {

                       "features": {

                           "graphics": {

                               "jpegSupport": true,
                               "h264Support" : {

                                    "enabled": true,
                                    "losslessOverlays": true,
                                    "dirtyRegions": true,
                                    "yuv444Support": false
                                }

                            }

                        }

                    }

         }

    }

 }


<!--NeedCopy-->
```

Lista de opciones de gráficos, junto con sus descripciones:

- “jpegSupport”: Disponibilidad de JPEG en gráficos (Thinwire).
- “h264Support”: Compatibilidad con el protocolo H.264.
- “enabled”: Disponibilidad de H.264 en Thinwire.
- “losslessOverlays”: Disponibilidad de superposiciones sin pérdida en Thinwire.
- “dirtyRegions”: Disponibilidad de regiones obsoletas en Thinwire.
- “yuv444Support”: Disponibilidad de Yuv444 en Thinwire.

> **Nota:**
>
> Recomendamos **inhabilitar** el **modo de gráficos antiguo**.

Limitaciones de la función

- La aplicación Citrix Workspace para ChromeOS no admite el modo de gráficos H.264 de pantalla completa para varios monitores.
- Cuando inicia una sesión de escritorio y abre una aplicación para introducir texto, cuando empieza a escribir, el texto desaparece y vuelve a aparecer. Puede notar que el texto parpadea. Este problema se produce cuando se utiliza el modo H.264 de pantalla completa.
- En una configuración de varios monitores, al abrir una aplicación publicada, se muestra una pantalla en blanco en lugar de la pantalla de la aplicación. Este problema se produce cuando se utiliza el modo H.264 de pantalla completa.

Selective H.264

Modo de configuración

Configuración de Selective H.264 en StoreFront mediante el archivo web.config Para cambiar la configuración de Selective H.264 mediante el archivo web.config:

1. Abra el archivo web.config del sitio de Citrix Receiver para Web.
   Este archivo se encuentra en la carpeta C:\inetpub\wwwroot\Citrix\<Storename>Web, donde *Storename* es el nombre que se especificó para el almacén cuando se creó.
2. Busque el campo **chromeAppPreferences** y establezca su valor con la configuración en forma de cadena JSON; por ejemplo:
   chromeAppPreferences='{"graphics":{"selectiveH264":false}}

Configuración de Selective H.264 mediante el archivo configuration.js El archivo **configuration.js** se encuentra en la **carpeta raíz de ChromeApp**. Modifique este archivo para modificar la aplicación Citrix Workspace según sus necesidades.

De manera predeterminada, Selective H.264 tiene el valor True.

Para inhabilitar la configuración de Selective H.264 mediante el archivo configuration.js:

1. Abra el archivo configuration.js y establezca el atributo selectiveH264 con el valor **false**.

```
'graphics': {
        'selectiveH264': false
}
```

> **Notas:**
>
> - Citrix recomienda hacer una copia de seguridad del archivo **configuration.js** antes de

> hacer cambios.
> - Citrix recomienda modificar el archivo **configuration.js** solo si la aplicación Citrix Workspace para ChromeOS se reempaqueta para los usuarios.
> - Se requieren credenciales de nivel de administrador para modificar el archivo **configuration.js**.

Otros (H.264)

Modo de configuración

Para configurar H.264, utilice la directiva de administración de Google para incluir lo siguiente. De forma predeterminada, la opción de la sección **other** está inhabilitada. Para habilitarla, establezca el atributo h264nonworker inhabilitado en true.

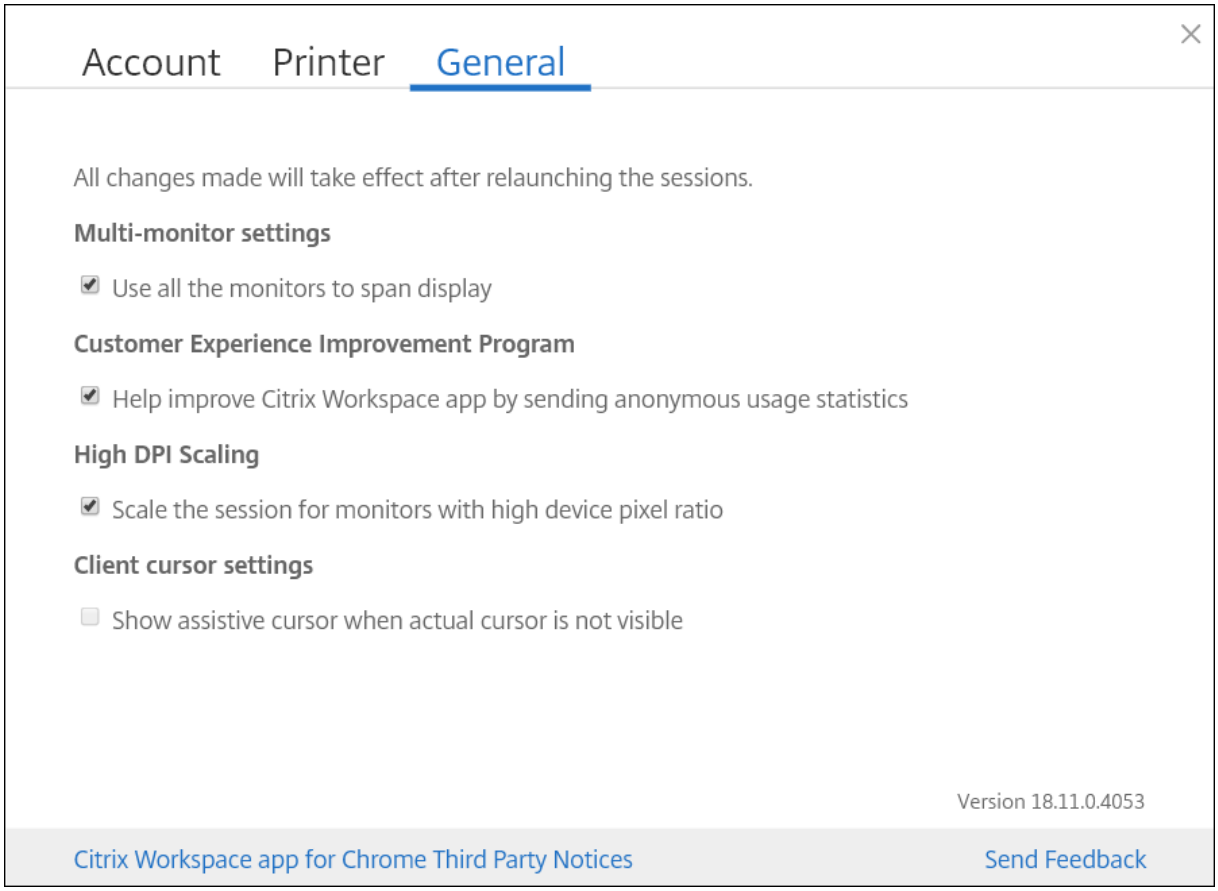
```
{

    "settings": {

        "Value": {

            "settings_version": "1.0",
                "engine_settings": {

                    "other": {

                        "h264nonworker" : false
                         }

                 }

          }

     }

 }


<!--NeedCopy-->
```

Lista de opciones, junto con sus descripciones:

- “h264nonworker”: Habilite la opción para decodificar H.264 en el subproceso principal.

Cursor de asistencia

Cuando el cursor no está visible dentro de una sesión de escritorio, puede habilitar un cursor de asistencia. Requiere reiniciar la sesión.



Modo de configuración

La función de cursor de asistencia está inhabilitada de forma predeterminada. Para habilitar la función del cursor de asistencia, utilice la directiva de administración de Google para incluir lo siguiente.

```
{

    "settings": {

        "Value": {

            "settings_version": "1.0",
            "engine_settings": {

                "ui": {

                    "assistiveCursor": true
                     }

                 }

```



```
17                }
18
19            }
20
21   }
22
23
24  <!--NeedCopy-->
```

Nota:

- Si un administrador habilita el cursor de asistencia como se ha descrito anteriormente, la casilla de verificación correspondiente en la configuración del lado del cliente se selecciona de forma predeterminada. Para inhabilitar la función, desmarque la casilla de verificación.
- Si un administrador inhabilita el cursor de asistencia como se ha descrito anteriormente, la casilla de verificación se desmarca y la función se inhabilita.

Escalado de PPP

Acerca de esta función

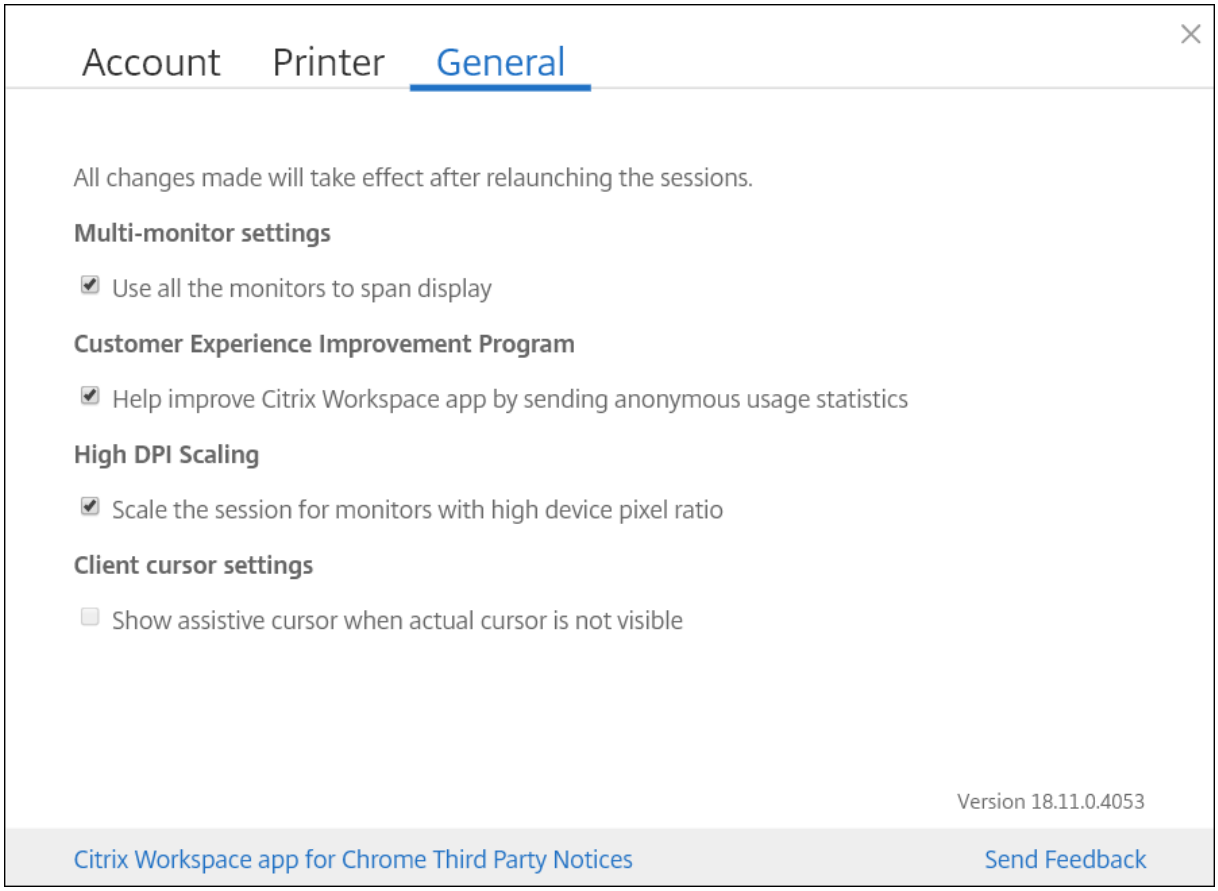
La aplicación Citrix Workspace para ChromeOS permite que el sistema operativo controle la resolución de las sesiones de escritorio y de aplicación, y admite el escalado de PPP en clientes para sesiones de aplicación en un solo monitor.

La aplicación Citrix Workspace para ChromeOS admite el escalado de PPP al permitirle establecer la resolución de VDA en monitores que tienen una alta proporción de píxeles.

La función **Escalado de PPP elevado** está inhabilitada de forma predeterminada para las sesiones de escritorio y aplicación. Para obtener una mejor resolución en dispositivos habilitados para PPP elevado, vaya a **Parámetros** y marque la casilla **Escalado de PPP elevado**.

Modo de configuración

Puede configurar el parámetro **Escalado de PPP elevado** únicamente mediante la directiva de Google Admin.



La función de escalado de PPP **Ajustar escala de la sesión en los monitores con proporción alta de píxeles** está habilitada de forma predeterminada.

Para establecer la resolución de las sesiones de escritorio, vaya a la barra de herramientas de la sesión. Seleccione **Preferencias** > **Resolución de pantalla** > **Usar ratio de píxeles del dispositivo** para que se establezca la resolución correcta en el VDA. Cuando la resolución se establece correctamente en el VDA, el texto borroso se vuelve nítido.

Para habilitar o inhabilitar la función, modifique la directiva de la **consola de administración de Google** y establezca el valor de **scaleToDPI** en **true** o en **false**.

Por ejemplo, para inhabilitar la función, establezca la propiedad **scaleToDPI** en **false**.

```
{

    "settings": {

                "Value": {

                        "settings_version": "1.0",
                              "engine_settings": {

       "features" : {

```



```
        "graphics" : {

                "dpiSetting": {

                                    "scaleToDPI": false
                                     }

                                }

                            }

                        }

                    }

                }

            }


<!--NeedCopy-->
```

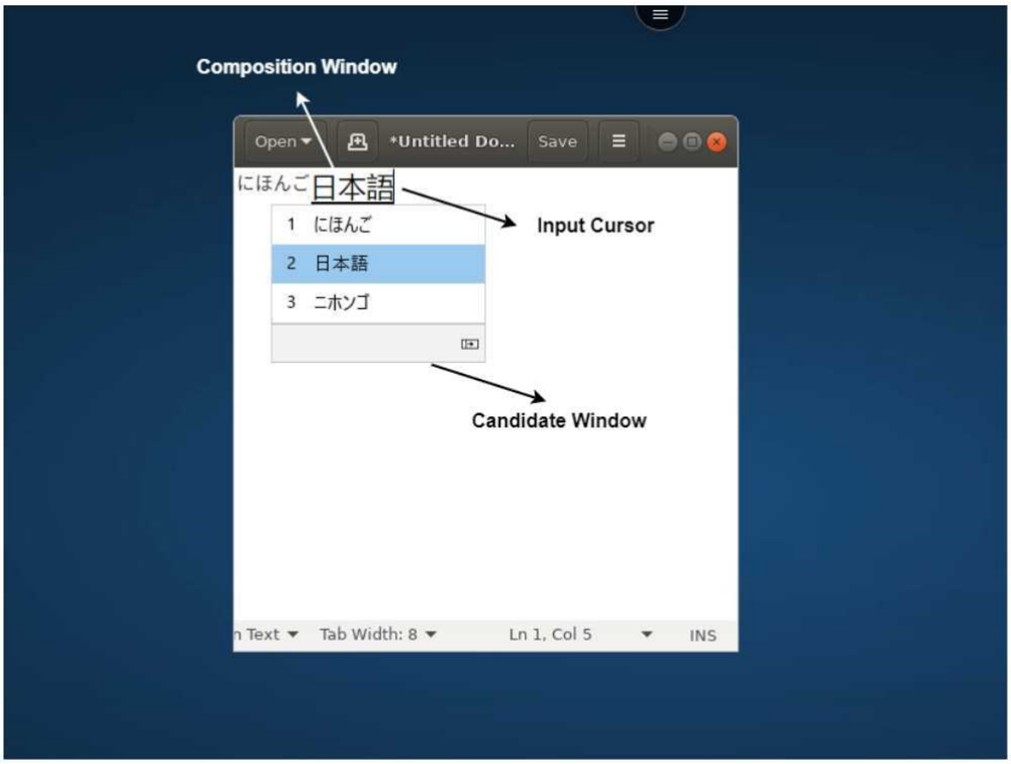
Teclado

May 16, 2024

IME de cliente genérico para idiomas de Asia Oriental

La función del editor de métodos de entrada (IME) de cliente genérico mejora la experiencia para escribir y ver caracteres en chino, japonés y coreano (CJK). Esta función le permite componer caracteres CJK en la posición del cursor cuando está en una sesión. La función está disponible para los entornos de Windows VDA y Linux VDA.

En general, el editor IME muestra componentes de interfaz de usuario como una ventana de candidatos y una ventana de redacción. La ventana de redacción incluye los caracteres redactados y los elementos de la interfaz de usuario de redacción. Por ejemplo, el subrayado y el color de fondo. La ventana de candidatos muestra la lista de candidatos.



La ventana de redacción le permite elegir entre los caracteres confirmados y los caracteres que se están escribiendo. La ventana de redacción y la ventana de candidatos se mueven con el cursor de entrada de texto. Como resultado, la función mejora la escritura de caracteres en la ubicación del cursor en la ventana de redacción. Además, ofrece una visualización mejorada en la composición y en la ventana de candidatos.

Requisitos previos:

- Para Linux VDA, habilite la directiva **Sincronización de la distribución del teclado del cliente y mejora de IME**.
- Para Windows VDA, habilite las directivas **Asignación de distribución de teclado Unicode**, **Sincronización de la distribución del teclado del cliente** y **Mejora de IME**.
- Utilice la versión 2012 de Citrix Linux VDA o una posterior. Para Citrix Windows VDA, todas las versiones de Windows VDA disponibles actualmente admiten la función IME de cliente genérico.
- El idioma del explorador web debe ser japonés, chino simplificado, chino tradicional o coreano.
- Use Google Chrome o Mozilla Firefox.

Limitaciones de la función:

- La composición de caracteres no funciona correctamente en celdas de Microsoft Excel. El problema ocurre al seleccionar la celda con un clic del mouse. [RFHTMCRM-6086]
- Ahora se admite el IME de cliente genérico cuando se usa una pantalla extendida. No obstante,

para las sesiones con varios monitores que aún no son compatibles, puede usar el **IME del servidor** en su lugar.

Para habilitar el **IME del servidor**:

1. Cambie el idioma del teclado del VDA o del servidor a chino, japonés o coreano (CJK), en función de lo que quiera.
2. Cambie el idioma del teclado del Chromebook a inglés.

Problema conocido de la función:

- Cuando Citrix IME no se agrega a la sesión de escritorio de un VDA, es posible que no pueda escribir los caracteres IME. El problema ocurre de forma intermitente en las versiones 2202 y anteriores del VDA. [HDX-36748]

Configuración:

A partir de la versión 2209, la función Generic Client IME está habilitada de forma predeterminada.

Como administrador, puede inhabilitar la función mediante el archivo **configuration.js** del servidor de StoreFront, que se halla normalmente en %ProgramFiles%\Citrix\Receiver StoreFront\HTML5Client. Para inhabilitar la función, vaya a **appPrefs** > **chromeApp** > **feature** > **ime** > configure **genericIME** como **false**.

Por ejemplo,

```
    "appPrefs":{

        "chromeApp":{

            "features" : {

                    "ime" : {

                    "genericIME": false
                }

       }

     }

     }

<!--NeedCopy-->
```

- Como administrador, puede inhabilitar la función mediante la consola de directivas de administración de Google al configurar **genericIME** como **false**.
  Por ejemplo,

```
    {
```



```
2
3     "settings": {
4
5     "Value": {
6
7       "settings_version": "1.0",
8       "engine_settings": {
9
10        "features": {
11
12          "ime": {
13
14            "genericIME": false
15           }
16
17         }
18
19       }
20
21      }
22
23      }
24
25  }
26
27  <!--NeedCopy-->
```

Accesos directos

Puede usar accesos directos estándar de Windows para copiar datos, como tablas de texto e imágenes, entre aplicaciones alojadas. Las aplicaciones alojadas pueden estar:

- En la misma sesión
- En sesiones diferentes

Solo se puede copiar y pegar texto Unicode sin formato entre las aplicaciones alojadas y el Portapapeles local del dispositivo.

Los usuarios pueden utilizar cualquier acceso directo estándar de teclado de Windows en la aplicación Citrix Workspace para ChromeOS porque estos accesos directos se transfieren de ChromeOS a las aplicaciones alojadas. Del mismo modo, también se pueden usar accesos directos únicos a aplicaciones específicas, siempre que no entren en conflicto con ningún acceso directo de ChromeOS.

Sin embargo, también se debe presionar la tecla **Windows** para que se reconozcan las teclas de función. Por lo tanto, se requiere un teclado externo. Para obtener más información sobre el uso de teclados de Windows con ChromeOS, consulte https://support.google.com/chromebook/answer/1047364. Los accesos directos específicos de Citrix, como los que se utilizan para cambiar de una sesión a otra y de una ventana a otra, no se pueden usar en la aplicación Citrix Workspace para ChromeOS.

Accesos directos de Excel

Modo de configuración

Los atajos de teclado se configuran con el atributo **sendAllKeys**.

Para que funcionen todos los accesos directos de Excel, configúrelos de la siguiente manera: **HTML5_CONFIG > features > sendAllKeys**

El atributo **sendAllKeys** está establecido en **true** de forma predeterminada. Para cambiar el valor predeterminado, abra el archivo **configuration.js**, agregue el atributo **sendAllKeys** y establezca el atributo en **false**.

Para obtener más información, consulte Cómo enviar directivas a través de la consola de administración de Google.

Compatibilidad con teclas de acceso directo y la tecla del logotipo de Microsoft Windows

> **Nota:**
>
> - En Chromebooks, utilice la tecla Buscar para asignar la tecla del logotipo de Microsoft Windows.

A partir de la versión 2108, se pueden usar la tecla del logotipo de Microsoft Windows y sus teclas de acceso directo en las sesiones de la aplicación Citrix Workspace para ChromeOS.

Ahora se pueden usar estas combinaciones de teclas:

- Windows + R
- Windows + D
- Windows + E
- Windows + M
- Windows + S
- Windows + CTRL + S
- Windows + T
- Windows + U
- Windows + Número
- Windows + X
- Windows + K

Visualización automática del teclado virtual

A partir de la versión 2211, aparece automáticamente un teclado virtual al colocar el cursor en un campo modificable. Esta función mejora la experiencia del usuario en dispositivos con pantalla táctil, a diferencia del comportamiento anterior, en el que había que hacer clic en el icono del teclado para ver el teclado virtual.

Modo de entrada de texto Scancode

La aplicación Citrix Workspace le permite utilizar teclados físicos externos para colaborar con la distribución del teclado del lado del servidor en el VDA. Cuando los administradores habilitan el modo Scancode, es posible que el usuario final utilice la distribución del teclado del servidor en lugar del cliente.

Esta función mejora la experiencia del usuario, especialmente cuando se usa un teclado físico en un idioma de Asia oriental.

> **Notas:**
>
> - De forma predeterminada, esta directiva de función está inhabilitada.
> - En los dispositivos táctiles, cuando la opción Scancode está habilitada, el teclado de software en pantalla no funciona desde la aplicación Citrix Workspace.

Configuración

Puede configurar el método de entrada Scancode de una de las siguientes maneras:

- Configuration.js
- Directiva administrativa de Google

Configuration.js

> **Notas:**
>
> - Citrix recomienda hacer una copia de seguridad del archivo **configuration.js** antes de hacer cambios.
> - Citrix recomienda modificar el archivo **configuration.js** solo si la aplicación Citrix Workspace para ChromeOS se reempaqueta para los usuarios.
> - Se requieren credenciales de nivel de administrador para modificar el archivo **configuration.js**.

Para habilitar la compatibilidad con el método de entrada de texto Scancode mediante el archivo **configuration.js**, haga lo siguiente:

1. Busque el archivo **configuration.js** en la carpeta raíz de ChromeApp.
2. Modifique el archivo y establezca el valor de **scancode** en **true**.

   A continuación se muestra un ejemplo de datos JSON:

```
"features" : {

        "ime": {

           "scancode": true,
         }

 }

<!--NeedCopy-->
```

3. Guarde los cambios.

Directiva administrativa de Google Para los usuarios y dispositivos administrados, los administradores pueden habilitar la función de compatibilidad con Scancode mediante la directiva administrativa de Google de esta manera:

1. Inicie sesión en la directiva administrativa de Google.
2. Vaya a **Administración de dispositivos** > **Administración de Chrome** > **Configuración de usuario**.
3. Agregue estas cadenas al archivo **policy.txt** en la clave engine_settings.

   > **Nota:**
   >
   > También puede aplicar esta configuración en lo siguiente:
   >
   > - **Dispositivo** > **Chrome** > **Aplicaciones y extensiones** > **Quioscos** > Buscar la extensión > Política de extensiones.
   > - **Dispositivo** > **Chrome** > **Aplicaciones y extensiones** > **Sesiones de invitados gestionadas** > Buscar la extensión > Política de extensiones.

   A continuación se muestra un ejemplo de datos JSON:

```
"features" :
{

    "ime": {

                "scancode": true
            }

 }

```



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

4. Guarde los cambios.

Asignación de teclado personalizada

A partir de la versión 2309, los usuarios finales pueden usar accesos directos y combinaciones de teclas específicos de Windows cuando el VDA es una máquina con sistema operativo Windows y el dispositivo de entrada nativo es un teclado ChromeOS. Ahora puede asignar las teclas **Ctrl** y **Alt** de forma personalizada. El usuario puede seleccionar la tecla Control (Ctrl) derecha o izquierda para que actúe como tecla Alt.

> **Notas:**
>
> - Esta asignación solo es posible en el modo de pantalla completa.
> - Tras guardar la configuración, la asignación afecta a todas las sesiones.
> - Esta función está activada de forma predeterminada.

Configuración

Puede configurar la asignación de teclado personalizada de una de las siguientes maneras:

- Configuration.js
- Directiva administrativa de Google

Configuration.js

> **Notas:**
>
> - Citrix recomienda hacer una copia de seguridad del archivo **configuration.js** antes de hacer cambios.
> - Citrix recomienda modificar el archivo **configuration.js** solo si la aplicación Citrix Workspace para ChromeOS se reempaqueta para los usuarios.
> - Se requieren credenciales de nivel de administrador para modificar el archivo **configuration.js**.

Para inhabilitar la función mediante el archivo **configuration.js**, haga lo siguiente:

1. Busque el archivo **configuration.js** en la carpeta raíz de ChromeApp.
2. Modifique el archivo y establezca el valor de **CustomKeyboardMapping** en **false**.

   A continuación se muestra un ejemplo de datos JSON:


```
"features" : {

        "ime": {

           "CustomKeyboardMapping": false,
         }

 }

<!--NeedCopy-->
```

3. Guarde los cambios.

Directiva administrativa de Google Para los usuarios y dispositivos administrados, los administradores pueden habilitar la función mediante la directiva administrativa de Google de esta manera:

1. Inicie sesión en la directiva administrativa de Google.
2. Vaya a **Administración de dispositivos** > **Administración de Chrome** > **Configuración de usuario**.
3. Agregue estas cadenas al archivo **policy.txt** en la clave engine_settings.

   > **Notas:**
   >
   > También puede aplicar esta configuración en lo siguiente:
   >
   > - **Dispositivo** > **Chrome** > **Aplicaciones y extensiones** > **Quioscos** > Buscar la extensión > Política de extensiones.
   > - **Dispositivo** > **Chrome** > **Aplicaciones y extensiones** > **Sesiones de invitados gestionadas** > Buscar la extensión > Política de extensiones.

   A continuación se muestra un ejemplo de datos JSON:

```
"features" :
{

    "ime": {

                "CustomKeyboardMapping": false
            }

 }

<!--NeedCopy-->
```

4. Guarde los cambios.

Para obtener más información sobre cómo utilizar esta función, consulte el artículo de la documentación de ayuda.

Uso de los accesos directos del sistema en el VDA en el modo de pantalla completa

A partir de la versión 2309, la aplicación Citrix Workspace en los dispositivos ChromeOS permite pasar los accesos directos del sistema al VDA (sesión de escritorio remoto) en modo de pantalla completa. Sin embargo, no surte efecto en el sistema operativo del cliente.

Anteriormente, estas combinaciones funcionaban a nivel local. Ahora, cuando la función está habilitada y en modo de pantalla completa, estas combinaciones se envían al VDA, aunque no se aplican localmente. Por ejemplo, una tecla **Actualizar** es una tecla del sistema en el Chromebook y la combinación **Ctrl+Mayús+Actualizar** es un acceso directo del sistema en ChromeOS para girar la pantalla. Sin embargo, el VDA Windows no realiza ninguna acción, puesto que no existe ese acceso directo en el sistema operativo Windows.

Otro ejemplo: `Alt`+[sirve para acoplar una ventana de ChromeOS a la izquierda, pero el mismo acceso directo no tiene ningún efecto en un VDA Windows. Algunas aplicaciones pueden usar estos accesos directos para una función específica; por ejemplo, algunos escáneres de códigos de barras usan `Alt`+[como prefijo.

> **Nota:**
>
> - Esta función está habilitada de manera predeterminada.

Las combinaciones de teclas son las siguientes:

Combinación de teclas de acceso directo	Acción en ChromeOS
Acción en ChromeOS	Cerrar sesión
Ctrl+Mayús+Actualizar	Girar la pantalla 90 grados
Ctrl+Mayús+L	Bloquear Chromebook
Alt+[	Acoplar una ventana a la izquierda
Alt+]	Acoplar una ventana a la derecha, teclas en el lateral, acoplar y restaurar ventanas.
Alt+”-“	Minimizar la ventana
Alt+”+”	Maximizar la ventana

> **Nota:**
>
> - Es posible que estos accesos directos del sistema no funcionen igual en el VDA, ya que estas combinaciones de teclas son accesos directos del sistema ChromeOS.

Configuración

Puede configurar la función de una de estas maneras:

- Configuration.js
- Directiva administrativa de Google

Configuration.js

> **Notas:**
>
> - Citrix recomienda hacer una copia de seguridad del archivo **configuration.js** antes de hacer cambios.
> - Citrix recomienda modificar el archivo **configuration.js** solo si la aplicación Citrix Workspace para ChromeOS se reempaqueta para los usuarios.
> - Se requieren credenciales de nivel de administrador para modificar el archivo **configuration.js**.

Para inhabilitar la función mediante el archivo **configuration.js**, haga lo siguiente:

1. Busque el archivo **configuration.js** en la carpeta raíz de ChromeApp.
2. Modifique el archivo y establezca el valor de **sendSysShortcutForFullScreen** en **false**.

   A continuación se muestra un ejemplo de datos JSON:

```
"features" : {

        "ime": {

           "sendSysShortcutForFullscreen": false,
         }

 }

<!--NeedCopy-->
```

3. Guarde los cambios.

Directiva administrativa de Google Para los usuarios y dispositivos administrados, los administradores pueden inhabilitar la función mediante la directiva de administración de Google de esta manera:

1. Inicie sesión en la directiva administrativa de Google.
2. Vaya a **Administración de dispositivos** > **Administración de Chrome** > **Configuración de usuario**.
3. Agregue estas cadenas al archivo **policy.txt** en la clave engine_settings.

   > **Notas:**
   >
   > También puede aplicar esta configuración en lo siguiente:
   >
   > - **Dispositivo** > **Chrome** > **Aplicaciones y extensiones** > **Quioscos** > Buscar la extensión > Política de extensiones.
   > - **Dispositivo** > **Chrome** > **Aplicaciones y extensiones** > **Sesiones de invitados gestionadas** > Buscar la extensión > Política de extensiones.

   A continuación se muestra un ejemplo de datos JSON:

```
"features" :
{

    "ime": {

                "sendSysShortcutForFullscreen": false
            }

 }

<!--NeedCopy-->
```

4. Guarde los cambios.

Licencias

May 16, 2024

ID de recurso

Acerca de esta función

La aplicación Citrix Workspace para Chrome utiliza un ID de recurso que los administradores configuran a través de la consola de administración de Google como nombre de cliente para las sesiones iniciadas desde Chromebooks inscritos.

Modo de configuración

De forma predeterminada, la aplicación Citrix Workspace sigue generando un ID de cliente único para los Chromebooks inscritos, el cual es similar a las versiones anteriores. Para utilizar esta función, debe establecer una directiva para la aplicación Citrix Workspace.

El valor de datos que introduzca no puede tener más de 15 caracteres. Los valores de más de 15 caracteres quedan cortados a los 15 caracteres.

Configurar el ID de recurso

1. Inicie una sesión en la Consola de administración de Google.
2. Vaya a `Device Management` > `Chrome` > `Devices Console` y agregue `Asset ID` para el dispositivo.
3. Modifique la directiva `Google Admin Console` y establezca el valor de `useAssetID` en **`true`**. De forma predeterminada, `useAssetID` se establece en **`false`**.

```
{

"settings": {

"Value": {

  "settings_version": "1.0",
  "engine_settings": {

    "uniqueID": {

      "useAssetID": true
                  }

              }

          }

      }

 }


<!--NeedCopy-->
```

Limitaciones de la función:

- Debe tener una directiva de administración de Google que se pueda enviar. De lo contrario, se sigue empleando el método actual de generación de un ID de cliente único para Chromebooks administrados.

- No introduzca un valor que tenga más de 15 caracteres. Los valores de más de 15 caracteres quedan cortados a los 15 caracteres.

ID único e ID de recurso

Se aplica un ID único como prefijo al nombre del cliente.

La aplicación Citrix Workspace para Chrome utiliza un ID de recurso que los administradores configuran a través de la **Consola de administración de Google** como nombre de cliente para las sesiones iniciadas desde Chromebooks inscritos.

Modo de configuración

Para configurar un ID de recurso desde la GUI, vaya a **Device Management** > **Chrome** > **Devices Console** y agregue el **ID de recurso** del dispositivo.

Para configurar manualmente un ID de recurso y un ID único, utilice la directiva de administración de Google para incluir lo siguiente:

```
{

    "settings": {

        "Value": {

            "settings_version": "1.0",
                "engine_settings": {

                        "uniqueID" : {

                                "prefixKey" : "CR-",
                                "restrictNameLength" : true,
                                "useAssetID": false
                                    }

                                  }

          }

     }

 }


<!--NeedCopy-->
```

Lista de opciones de uniqueID, junto con sus descripciones:

- "prefixKey": El prefijo que se utilizará antes del nombre del cliente. El valor predeterminado es CR.
- "restrictNameLength": Habilita o inhabilita la longitud del nombre de prefixKey.
- "useAssetID": El ID de recurso que se establece como nombre de cliente para las sesiones iniciadas desde Chromebooks inscritos.

Limitaciones de la función:

- Debe tener una directiva de administración de Google que se pueda enviar. De lo contrario, se sigue empleando el método actual de generación de un ID de cliente único para Chromebooks administrados.
- No introduzca un valor que contenga más de 15 caracteres. Los valores de más de 15 caracteres quedan cortados a los 15 caracteres.

Contenido multimedia

May 16, 2024

Audio

Puede utilizar auriculares USB en una sesión para poder hablar y escuchar. También puede usar los botones de los auriculares USB (como silenciar y omitir). La experiencia del usuario se enriquece al proporcionar una salida de audio fluida.

Audio adaptable

Con el audio adaptable, no es necesario configurar las directivas de calidad de audio en los VDA. El audio adaptable optimiza los parámetros de su entorno. Reemplaza los formatos antiguos de compresión de audio para ofrecer una excelente experiencia de usuario.

Para obtener más información, consulte Audio adaptable en la documentación de Citrix Virtual Apps and Desktops.

Atributos de función

Hay dos atributos de función:

- **EnableAdaptiveAudio:** Establezca el valor en true para habilitar la función de audio adaptable. Establezca el valor en false para inhabilitar la función.

- **EnableStereoRecording:** La grabación en estéreo es una función opcional. De forma predeterminada, esta función está inhabilitada. Establezca el valor del atributo **EnableStereoRecording** en **true** para habilitar la grabación estéreo o establezca el valor en **false** para inhabilitar la función. Esta función solo está disponible cuando la función de audio adaptable está habilitada. Si el atributo **EnableStereoRecording** se establece en true, la grabación en estéreo está disponible con la eliminación de eco inhabilitada.

Modo de configuración

Puede configurar la función de audio adaptable de estas maneras:

- Configuration.js
- Directiva administrativa de Google

Configuration.js Para configurar el audio adaptable mediante el archivo **configuration.js**, haga lo siguiente:

1. Busque el archivo **configuration.js** en la carpeta **raíz de ChromeApp**.
2. Modifique este archivo para configurar la función de audio adaptable.

   > **Notas:**
   >
   > - Citrix recomienda hacer una copia de seguridad del archivo **configuration.js** antes de hacer cambios.
   > - Citrix recomienda modificar el archivo **configuration.js** solo si la aplicación Citrix Workspace para ChromeOS se reempaqueta para los usuarios.
   > - Se requieren credenciales de nivel de administrador para modificar el archivo **configuration.js**.

3. Establezca el valor predeterminado de **EnableAdaptiveAudio** en **true**. Establezca el valor predeterminado de **EnableStereoRecording** en **false**.

   A continuación se muestra un ejemplo de datos JSON:

```
"features" : {

    "audio" : {

    "EnableAdaptiveAudio": true
             }

 }


"features" : {
```



```
12
13      "audio" : {
14
15          "EnableStereoRecording": false
16               }
17
18   }
19
20  <!--NeedCopy-->
```

4. Guarde los cambios.

> **Nota:**
>
> - Para inhabilitar la función, establezca el atributo **EnableAdaptiveAudio** en **false**.

Directiva administrativa de Google En la implementación local, los administradores pueden habilitar la función de audio adaptable mediante la directiva administrativa de Google de la siguiente manera:

1. Inicie sesión en la directiva administrativa de Google.
2. Vaya a **Administración de dispositivos** > **Administración de Chrome** > **Configuración de usuario**.
3. Agregue estas cadenas al archivo **policy.txt** en la clave **engine_settings**.

   A continuación se muestra un ejemplo de datos JSON:

```
1  "features" : {
2
3      "audio" : {
4
5          "EnableAdaptiveAudio": {
6
7              "type": "boolean" }
8
9                      }
10
11                 }
12
13
14 "features" : {
15
16     "audio" : {
17
18         "EnableStereoRecording": {
19
20             "type": "boolean" }
21
22                 }
```



```
23
24                  }
25
26  <!--NeedCopy-->
```

4. Guarde los cambios.

Compatibilidad con dispositivos de audio Plug and Play

Antes, solo se admitía un único dispositivo de reproducción y grabación de audio, y se mostraba como **Citrix HDX Audio**, independientemente del nombre real del dispositivo.

A partir de la versión 2301, admitimos varios dispositivos de audio y los redirigimos a VDA. Ahora, al redirigir dispositivos de audio, puede ver el nombre real del dispositivo de audio en Parámetros de **sonido** > Parámetros de **reproducción** y **sonido** > **Grabación** en el VDA. La lista de dispositivos del VDA se actualiza dinámicamente cada vez que se conecta o se quita un dispositivo de audio.

> **Nota:**
>
> De manera predeterminada, esta función está habilitada.

Configuración

Puede configurar esta función de una de estas maneras:

- Configuration.js
- Directiva administrativa de Google

Configuration.js Para inhabilitar la compatibilidad de dispositivos de audio Plug and Play mediante el archivo **configuration.js**, haga lo siguiente:

1. Busque el archivo **configuration.js** en la carpeta **raíz de ChromeApp**.
2. Modifique el archivo para configurar la función de compatibilidad con dispositivos de audio Plug and Play.

   > **Notas:**
   >
   > - Citrix recomienda hacer una copia de seguridad del archivo **configuration.js** antes de hacer cambios.
   > - Citrix recomienda modificar el archivo **configuration.js** solo si la aplicación Citrix Workspace para ChromeOS se reempaqueta para los usuarios.
   > - Se requieren credenciales de nivel de administrador para modificar el archivo **configuration.js**.

3. Establezca el valor de **AudioRedirectionV4** en **false**. A continuación se muestra un ejemplo de datos JSON:

```
    "features" : {

        "audio" : {

          "AudioRedirectionV4": false
                }

         }

<!--NeedCopy-->
```

4. Guarde los cambios.

Directiva administrativa de Google En la implementación local, los administradores pueden inhabilitar la función de dispositivos de audio Plug and Play mediante la directiva administrativa de Google de esta manera:

1. Inicie sesión en la directiva administrativa de Google.
2. Vaya a **Administración de dispositivos** > **Administración de Chrome** > **Configuración de usuario**.
3. Agregue estas cadenas al archivo **.txt**, en la clave **engine_settings**.

   A continuación se muestra un ejemplo de datos JSON:

```
    "features" : {

        "audio" : {

          "AudioRedirectionV4": false
                }

         }

<!--NeedCopy-->
```

4. Guarde los cambios.

Limitaciones conocidas

- En el VDA, el nombre del dispositivo de audio integrado solo está en inglés. El problema se produce al usar dispositivos basados en ChromeOS. [RFHTMCRM-8667]

Cámara web

La aplicación Citrix Workspace para ChromeOS ofrece una mejora para la redirección de cámaras web. La codificación por hardware H.264 para cámaras web ayuda a reducir la carga de CPU e incrementa la eficiencia de la batería de los dispositivos Chromebook. Estos dispositivos tienen codificadores para H.264, que aprovecha la funcionalidad de Intel en la API de PPB_VideoEncoder.

La aplicación Citrix Workspace para ChromeOS ofrece la redirección de cámaras web tanto para aplicaciones de 32 bits como de 64 bits.

Redirección de cámaras web

La redirección de cámara web está disponible para aplicaciones de 32 bits y 64 bits. La redirección de cámara web en aplicaciones de 32 bits y 64 bits está limitada a cámaras web integradas.

Ahora puede utilizar cámaras web externas en sesiones de aplicaciones y escritorios virtuales de la aplicación Citrix Workspace para ChromeOS. La aplicación Citrix Workspace detecta cámaras web externas recién conectadas y las habilita para su uso de manera dinámica.

Modo de configuración

Configure la redirección de cámara web para 64 bits de la siguiente manera:

Configurar la cámara web mediante el archivo configuration.js y la consola de administración de Google Para 2101 y las versiones posteriores:

Configure la redirección de cámara web con la siguiente ruta: **HTML5_CONFIG > features > video**

> **Nota:**
>
> Se recomienda utilizar la ruta **HTML5_CONFIG > features > video** para configurar la redirección de cámara web. La otra ruta funcionará durante algún tiempo, pero se eliminará en una versión futura.

Recomendaciones para la redirección de cámara web

- Establezca la directiva Calidad de sonido de Citrix Delivery Controller en Baja o Media. Si utiliza Chromebooks de baja potencia, es posible que se produzcan retrasos de audio si no configura la directiva Calidad de sonido.
- Para obtener el mejor rendimiento, se recomienda utilizar Chromebooks de gama alta y redes de baja latencia con conexiones de buen ancho de banda.

- Establezca la siguiente clave de Registro en un VDA:

  HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\HdxRealTime

  Nombre: OfferH264ToApp

  Tipo: REG_DWORD

  Valor: 1

> **Nota:**
>
> Esta configuración se aplica a los usuarios actuales. Para los usuarios nuevos, establezca la clave de Registro mediante el Editor de objetos de directiva de grupo (GPO) de Windows.

RENUNCIA DE RESPONSABILIDADES: ¡Precaución! El uso incorrecto del Editor del Registro del sistema puede causar problemas graves que pueden obligarle a reinstalar el sistema operativo. Citrix no puede garantizar que los problemas derivados de la utilización inadecuada del Editor del Registro puedan resolverse. Use el Editor del Registro bajo su propia responsabilidad. Haga una copia de seguridad del Registro antes de modificarlo.

Optimización de Microsoft Teams

May 16, 2024

Ahora puede utilizar estas funciones de Microsoft Teams para las sesiones de escritorios virtuales y de aplicaciones virtuales:

- Llamadas de audio optimizadas
- Videollamadas optimizadas
- Uso compartido de la pantalla optimizado

Solo está disponible en la versión 1906 de VDA y posteriores.

> **Notas:**
>
> - De forma predeterminada, el uso compartido de la pantalla permite compartir toda la pantalla. Sin embargo, solo puede limitar el uso compartido de la pantalla del contenido de la aplicación Citrix Workspace. Para obtener más información, consulte Limitar el uso compartido de la pantalla del contenido de la aplicación Citrix Workspace. Para habilitar la función del uso compartido de la pantalla a través de la directiva administrativa de Google, consulte Parámetros de optimización de Microsoft Teams.
> - Para solucionar problemas y cambiar Microsoft Teams del modo no optimizado al modo

> optimizado en la sesión de cliente, consulte Solución de problemas para la optimización de Microsoft Teams.
>
> - Durante el uso compartido de la pantalla mediante la optimización de Microsoft Teams, el borde rojo de la ventana compartida no aparece.
> - No se pueden compartir aplicaciones.
> - La optimización de Microsoft Teams para llamadas de audio, vídeo y pantalla compartida está disponible de forma general a partir de la versión 2105.5. Le recomendamos actualizar su versión a la versión más reciente de la aplicación Citrix Workspace para ChromeOS.

Videollamadas y uso compartido de la pantalla en monitores externos

En su monitor externo, ahora puede utilizar estas funciones de Microsoft Teams durante las llamadas.

- Vídeo optimizado
- Uso compartido de la pantalla optimizado

Estas funciones están disponibles para llamadas de Microsoft Teams dentro de escritorios virtuales. También están disponibles para llamadas realizadas a través de la aplicación virtual de Microsoft Teams al colocar las ventanas de Microsoft Teams en un monitor externo.

Notas (actualización de la versión 96 de ChromeOS)

- Para evitar que la actualización de la versión 96 de ChromeOS afecte al funcionamiento de Microsoft Teams, haga esto antes de actualizar ChromeOS:
- Para los usuarios de una versión reempaquetada de la aplicación Citrix Workspace, consulte el artículo CTX331648 de Knowledge Center e implemente los pasos.
- Para todos los demás usuarios de la versión 2110 de la aplicación Citrix Workspace para ChromeOS y anteriores, consulte el artículo CTX331653 de Knowledge Center.

Parámetros de optimización de Microsoft Teams

Para habilitar el uso compartido de la pantalla

Para habilitar el uso compartido de la pantalla mediante la directiva administrativa de Google, cambie a **true** el valor de **msTeamsOptimization** de esta manera.

Para obtener más información, consulte el artículo Cómo enviar directivas a través de la consola de administración de Google.


```
{

  "settings": {

     "Value": {

       "settings_version": "1.0",
          "engine_settings": {

              "features":{

                 "msTeamsOptimization":{

                 "screenSharing" : true
                    }

                 }

              }

           }

       }

   }


<!--NeedCopy-->
```

Para habilitar el uso compartido de la pantalla para usuarios con sus propios dispositivos o BYOD (solo para los que usen instancias locales de StoreFront):

Siga los pasos descritos en el artículo Mediante web.config y agregue el **valor de chromeAppPreferences** de esta manera:

Por ejemplo:

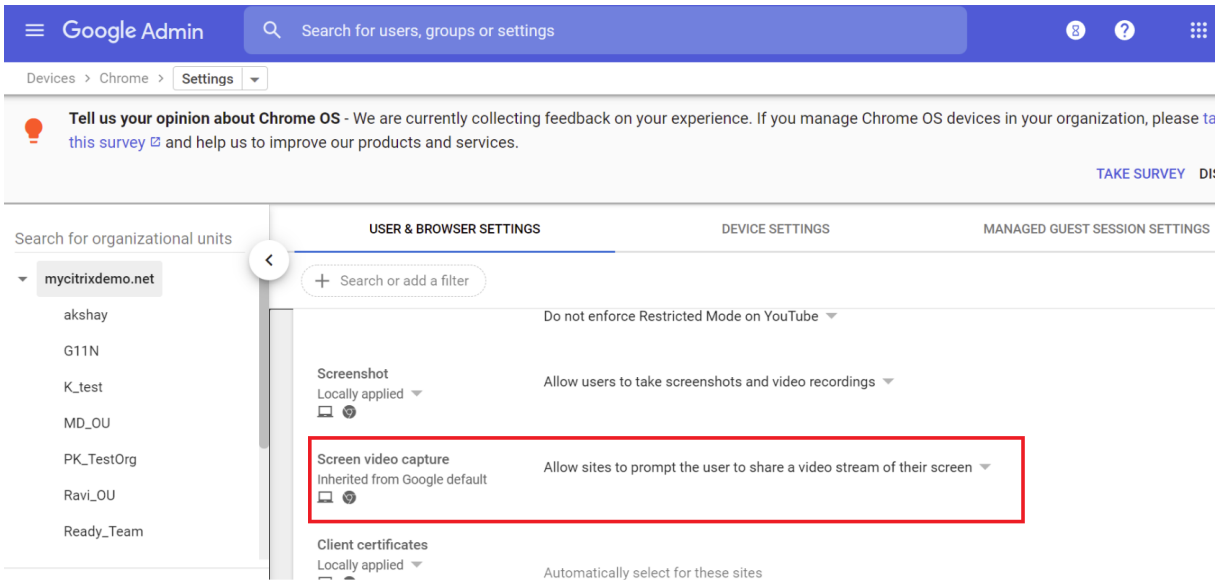
```
chromeAppPreferences = {

    "features":{

        "msTeamsOptimization":{

            "screenSharing":true
             }

             }

             }

<!--NeedCopy-->
```


Parámetros en la consola de administración de Google

Asegúrese de que los siguientes parámetros estén permitidos en la **Consola de administración de Google** para que funcione la optimización del uso compartido de la pantalla.

En la **Consola de administración de Google**, en **Dispositivos** > **Chrome** > **Configuración**, seleccione > **Permitir que los sitios pidan al usuario que comparta una secuencia de vídeo de su pantalla** en **Captura de pantalla de vídeo** para las tres categorías:

- **Configuración de usuario y explorador**
- **Parámetros del dispositivo**
- **Configuración de sesión de invitado gestionada** (o una categoría adecuada).



Limitar el uso compartido de la pantalla del contenido de la aplicación Citrix Workspace

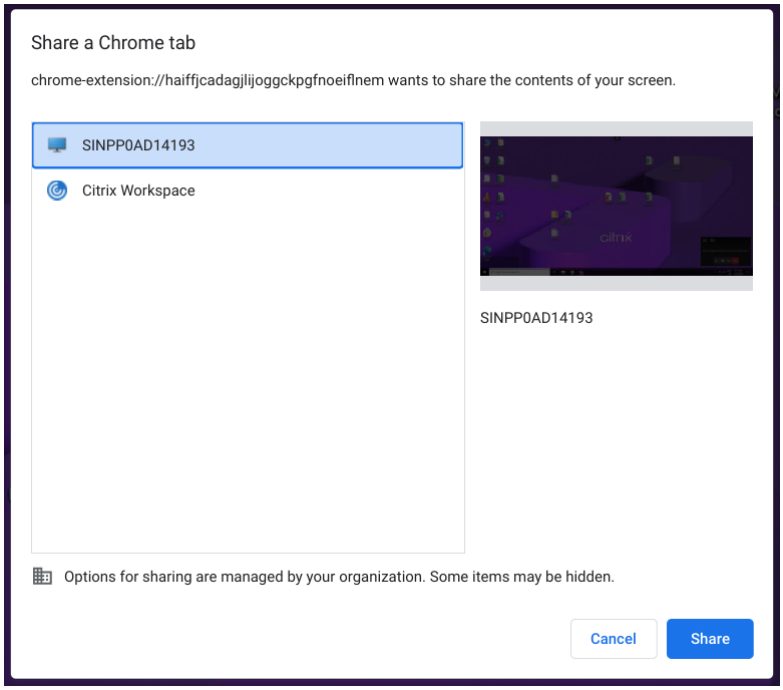
Para la optimización de Microsoft Teams, los administradores pueden limitar el uso compartido de la pantalla de aplicaciones y escritorios que solo se abren a través de la aplicación Citrix Workspace en dispositivos Chrome administrados.
Cuando los administradores activan esta función, los usuarios finales pueden compartir recursos que se hayan abierto solamente desde la aplicación Citrix Workspace.

Esta función está disponible a partir de la versión M98 de Chrome.

Para configurar los parámetros, utilice las directivas de Google de la siguiente manera:

1. Vaya a la **Consola de administración de Google** > **Settings** > **User & browser settings**.

2. Vaya a **Screen video capture allowed by sites** > **Allow tab video capture (same site only) by these sites** e introduzca el ID de aplicación de la aplicación Citrix Workspace para ChromeOS -haiffjcadagjlijoggckpgfnoeiflnem.

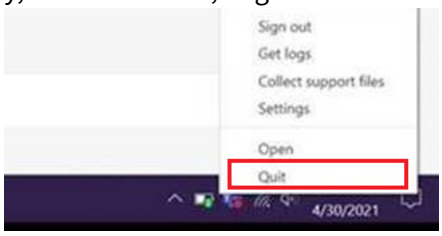


A partir de ahora, los usuarios finales solo podrán seleccionar la ficha y compartir contenido abierto a través de la aplicación Citrix Workspace.

Solución de problemas para la optimización de Microsoft Teams

Para cambiar Microsoft Teams de un estado no optimizado al optimizado dentro de las sesiones de cliente, haga lo siguiente:

- Haga clic con el botón secundario en el icono de Microsoft Teams para salir de Microsoft Teams y, a continuación, haga clic en **Cerrar**. Inicie Microsoft Teams de nuevo.



- Si el cierre no funciona, cierre la sesión e iníciela de nuevo.
- Si no funciona el hecho de cerrar sesión y volver a iniciarla, borre la caché en el directorio **C:\Usuarios\Administrator\AppData\Roaming\Microsoft\Teams** en el VDA y, a continuación, reinicie Microsoft Teams.

Para obtener más información, consulte Solucionar problemas.

Para solucionar problemas en la versión de biblioteca de correcciones de compatibilidad, consulte la sección Registros de la optimización de Microsoft Teams.

Compatibilidad con e911 dinámico

La aplicación Citrix Workspace admite llamadas de emergencia dinámicas. Cuando se usa en los planes de llamadas de Microsoft, Operator Connect y enrutamiento directo, proporciona la capacidad de:

- configurar y redirigir llamadas de emergencia
- notificar al personal de seguridad

La notificación se proporciona en función de la ubicación actual de la aplicación Citrix Workspace que se ejecuta en el dispositivo de punto final, en lugar del cliente de Microsoft Teams del VDA.

La ley de Ray Baum exige que la ubicación transmitible de la persona que llama al 911 se transmita al Punto de Respuesta de Seguridad Pública (PSAP) correspondiente. A partir de la aplicación Citrix Workspace 2112 para ChromeOS, Optimización para Microsoft Teams con HDX cumple con la ley de Ray Baum.

Desenfoque de fondo y efectos en la optimización de Microsoft Teams

A partir de la versión 2303, la aplicación Citrix Workspace para ChromeOS admite el desenfoque de fondo y los efectos en la optimización de Microsoft Teams para videollamadas. Puede difuminar o reemplazar los efectos de fondo que proporciona Microsoft Teams. Esta función sirve para evitar distracciones inesperadas, ayudando a que la conversación se centre en la silueta (cuerpo y rostro). Esta función se puede utilizar con llamadas de conferencia y entre dos usuarios.

> **Notas:**
>
> - De forma predeterminada, esta función está inhabilitada.
> - Ahora, esta función está integrada en los botones y la interfaz de usuario de Microsoft Teams. La compatibilidad con varias ventanas es un requisito previo que necesita una actualización de VDA a la versión 2112 o a una posterior. Para obtener más información, consulte Reuniones y chat en modo multiventana.

Limitaciones

- No se permite el reemplazo de fondos definido por el administrador ni por el usuario.
- Al habilitar esta función, es posible que note problemas de rendimiento.

- Cuando la sesión ICA se conecta de nuevo, el efecto está desactivado. Sin embargo, la interfaz de usuario de Microsoft Teams muestra que el efecto anterior sigue activado con una marca de verificación. Citrix y Microsoft están trabajando juntos para resolver este problema.

Modo de configuración Puede habilitar la función de efectos de fondo de una de estas maneras:

- Configuration.js
- Directiva administrativa de Google
- Global App Configuration Service

Configuration.js Para configurar el desenfoque de fondo y los efectos de fondo mediante el archivo **configuration.js**, haga lo siguiente:

1. Busque el archivo **configuration.js** en la carpeta raíz de **ChromeApp**.

   > **Notas:**
   >
   > - Citrix recomienda hacer una copia de seguridad del archivo **configuration.js** antes de hacer cambios.
   > - Citrix recomienda modificar el archivo **configuration.js** solo si la aplicación Citrix Workspace para ChromeOS se reempaqueta para los usuarios.
   > - Se requieren credenciales de nivel de administrador para modificar el archivo **configuration.js**.

2. Modifique el archivo **configuration.js** y establezca el valor predeterminado de backgroundEffects en true.

   A continuación se muestra un ejemplo de datos JSON:

   ```
   "features" :
   {

       "msTeamsOptimization" : {

           "backgroundEffects" : true
        }

    }

   <!--NeedCopy-->
   ```

3. Guarde los cambios.

Directiva administrativa de Google En la implementación local, los administradores pueden habilitar la función de efectos de fondo mediante la directiva administrativa de Google de la siguiente manera:

1. Inicie sesión en la directiva administrativa de Google.
2. Vaya a **Administración de dispositivos** > **Administración de Chrome** > **Configuración de usuario**.
3. Agregue estas cadenas al archivo **policy.txt** en la clave **engine_settings**.
   A continuación se muestra un ejemplo de datos JSON:

```
"features" :
{

    "msTeamsOptimization" : {

        "backgroundEffects" : true
     }

 }

<!--NeedCopy-->
```

4. Guarde los cambios.

Global App Configuration Service En la configuración en la nube, los administradores pueden habilitar la función de efectos de fondo al establecer el atributo **backgroundEffects** en **True** en Global App Configuration Service.

Para obtener más información, consulte la documentación de Global App Configuration Service.

Multifrecuencia de doble tono (DTMF) con Microsoft Teams

Ahora, la aplicación Citrix Workspace ofrece la interacción de marcado con multifrecuencia de doble tono (DTMF) en sistemas de telefonía (por ejemplo, PSTN) y llamadas de conferencia de Microsoft Teams. Esta función está habilitada de manera predeterminada.

Subtítulos en directo de Microsoft Teams

La optimización de Microsoft Teams admite la transcripción en tiempo real de lo que dice los ponentes cuando los subtítulos en directo están habilitados en Microsoft Teams.

Compatibilidad con timbre secundario

A partir de la versión 2312, puede usar la función de timbre secundario para seleccionar un dispositivo secundario en el que recibir la notificación de llamada entrante. Esta función solo es aplicable cuando Microsoft Teams está optimizado.

Por ejemplo, considere que ha establecido un altavoz como timbre secundario y que su dispositivo de punto final está conectado a los auriculares. En este caso, Microsoft Teams envía el timbre de la llamada entrante tanto a los auriculares como al altavoz. No se puede establecer un timbre secundario en los siguientes casos:

- Cuando no se ha conectado a más de un dispositivo de audio
- Si el periférico no está disponible (por ejemplo, auriculares Bluetooth con micrófono)

> **Nota**
>
> De forma predeterminada, esta función está inhabilitada.

Limitaciones conocidas de la función

- Al habilitar esta función, es posible que oiga el timbre secundario dos veces con una ligera demora. Este problema es un error de Microsoft Teams, y planean solucionarlo en la próxima versión de Microsoft Teams.

Configuración

Puede configurar la función de timbre secundario de una de estas maneras:

- Configuration.js
- Directiva administrativa de Google

Configuration.js

> **Notas:**
>
> Citrix recomienda hacer una copia de seguridad del archivo **configuration.js** antes de hacer cambios.
> Citrix recomienda modificar el archivo **configuration.js** solo si la aplicación Citrix Workspace para ChromeOS se reempaqueta para los usuarios.
> Se requieren credenciales de nivel de administrador para modificar el archivo **configuration.js**.

Para habilitar la función mediante el archivo **configuration.js**, haga lo siguiente:

1. Busque el archivo **configuration.js** en la carpeta raíz de ChromeApp.
2. Modifique el archivo y establezca el valor de **secondaryRingtone** en **true**.

   A continuación se muestra un ejemplo de datos JSON:

```
{

```



```
    "features":{

        "msTeamsOptimization":{

            "secondaryRingtone" : true
             }

         }

 }

<!--NeedCopy-->
```

3. Guarde los cambios.

Directiva administrativa de Google Para los usuarios y dispositivos administrados, los administradores pueden habilitar la función mediante la directiva administrativa de Google de esta manera:

1. Inicie sesión en la directiva administrativa de Google.
2. También puede aplicar esta configuración en lo siguiente:
   - **Dispositivo** > **Chrome** > **Aplicaciones y extensiones** > **Usuarios y exploradores** > busque la extensión > Política de extensiones.
   - **Dispositivo** > **Chrome** > **Aplicaciones y extensiones** > **Quioscos** > Buscar la extensión > Política de extensiones.
   - **Dispositivo** > **Chrome** > **Aplicaciones y extensiones** > **Sesiones de invitados gestionadas** > Buscar la extensión > Política de extensiones.

   A continuación se muestra un ejemplo de datos JSON:

```
      {

          "settings": {

                "Value": {

                   "settings_version": "1.0",
                     "engine_settings": {

                          "features":{

                                  "msTeamsOptimization":{

                                          "secondaryRingtone" :
                                             true  }

                                                  }
```



```
18                                                          }
19
20                                                  }
21
22                                          }
23
24                  }
25
26  <!--NeedCopy-->
```

3. Guarde los cambios.

Implementación de la transmisión simultánea para llamadas de videoconferencia de Microsoft Teams optimizado

A partir de la versión 2312, la función de transmisión simultánea está habilitada de forma predeterminada para las llamadas de videoconferencia en Microsoft Teams optimizado. Con esta compatibilidad, la calidad y la experiencia de las videoconferencias en diferentes dispositivos de punto final mejoran. Esto se logra al adaptarse a la resolución adecuada para ofrecer la mejor experiencia de llamadas para todos los usuarios.

Con esta experiencia mejorada, cada usuario puede emitir varias transmisiones de vídeo en diferentes resoluciones (por ejemplo, 720p, 360p, etc.). Las resoluciones dependen de varios factores, como la capacidad del punto final, las condiciones de la red, etc. El dispositivo de punto final receptor solicita entonces la resolución de máxima calidad que pueda gestionar. Por lo tanto, ofrece a todos los usuarios la experiencia de vídeo óptima.

Compatibilidad con la optimización para Zoom

May 16, 2024

A partir de la versión 2402.1, la aplicación Citrix Workspace para ChromeOS admite la integración con la solución de infraestructura de escritorio virtual (VDI) de Zoom para ofrecer una experiencia optimizada en las conferencias de audio y vídeo dentro de las sesiones.

> **Nota:**
>
> Esta función está habilitada de forma predeterminada; sin embargo, los administradores deben configurarla. Solo está disponible en la versión 1906 de VDA y posteriores.

Requisitos previos

Los administradores deben configurar:

- La directiva de DDC **VirtualChannelWhiteList** para usar los canales virtuales de Zoom. Para obtener más información, consulte Configuraciones de la directiva Lista de canales virtuales permitidos en la documentación de .
- Los requisitos previos para configurar la VDI de Zoom para ChromeOS.

Limitaciones de la función

- La ventana de visualización de conferencias de Zoom se limita únicamente al monitor principal.
- Los dispositivos HID no son compatibles
- Para ver otras limitaciones, consulte Limitations of using Zoom VDI for ChromeOS.

Modo de configuración

Puede configurar la función de una de estas maneras:

- Configuration.js
- Directiva administrativa de Google

Configuration.js

> **Notas:**
>
> - Citrix recomienda hacer una copia de seguridad del archivo **configuration.js** antes de hacer cambios.
> - Citrix recomienda modificar el archivo **configuration.js** solo si la aplicación Citrix Workspace para ChromeOS se reempaqueta para los usuarios.
> - Se requieren credenciales de nivel de administrador para modificar el archivo **configuration.js**.

Para configurar la función mediante el archivo **configuration.js**, haga lo siguiente:

1. Busque el archivo **configuration.js** en la carpeta raíz de ChromeApp.
2. Modifique el archivo **configuration.js** y agregue las URL de Zoom según sea necesario.

   A continuación se muestra un ejemplo de datos JSON:


```
"features" :
{

    "customVC": [
    {

        "streamName": "ZOOMHDX",
        "appId": "html=https://zoom.us/vdi/plugin"
     }
 ,
    {

        "streamName": "ZOOMHDC",
        "appId": "html=https://zoom.us/vdi/plugin"
     }
 ,
    {

        "streamName": "ZOOMPHX",
        "appId": "html=https://zoom.us/vdi/plugin"
     }

],
"customVCWhitelistURL": [
    {

        "url": "https://zoom.us/vdi/plugin",
        "permissions": [
            "media"
        ]
     }
 ,
    {

        "url": "https://zoom.us/vdi/webview",
        "permissions": [
            "media"
        ]
     }

]

 }

<!--NeedCopy-->
```

3. Guarde los cambios.

Directiva administrativa de Google

Para los usuarios y dispositivos administrados, los administradores pueden configurar la función mediante la directiva administrativa de Google de esta manera:

1. Inicie sesión en la directiva administrativa de Google.
2. Vaya a **Administración de dispositivos** > **Administración de Chrome** > **Configuración de usuario**.
3. Agregue estas cadenas al archivo **policy.txt** en la clave engine_settings.

   > **Nota:**
   >
   > También puede aplicar esta configuración en lo siguiente:
   >
   > - **Dispositivo** > **Chrome** > **Aplicaciones y extensiones** > **Usuarios y exploradores** > busque la extensión > Política de extensiones.
   > - **Dispositivo** > **Chrome** > **Aplicaciones y extensiones** > **Quioscos** > Buscar la extensión > Política de extensiones.
   > - **Dispositivo** > **Chrome** > **Aplicaciones y extensiones** > **Sesiones de invitados gestionadas** > Buscar la extensión > Política de extensiones.

   A continuación se muestra un ejemplo de datos JSON:

```
{

"settings": {

"Value": {

    "settings_version": "1.0",

"customVC": [
   {

       "streamName": "ZOOMHDX",
       "appId": "html=https://zoom.us/vdi/plugin"
    }
 ,
   {

       "streamName": "ZOOMHDC",
       "appId": "html=https://zoom.us/vdi/plugin"
    }
 ,
   {

       "streamName": "ZOOMPHX",
       "appId": "html=https://zoom.us/vdi/plugin"
    }
```



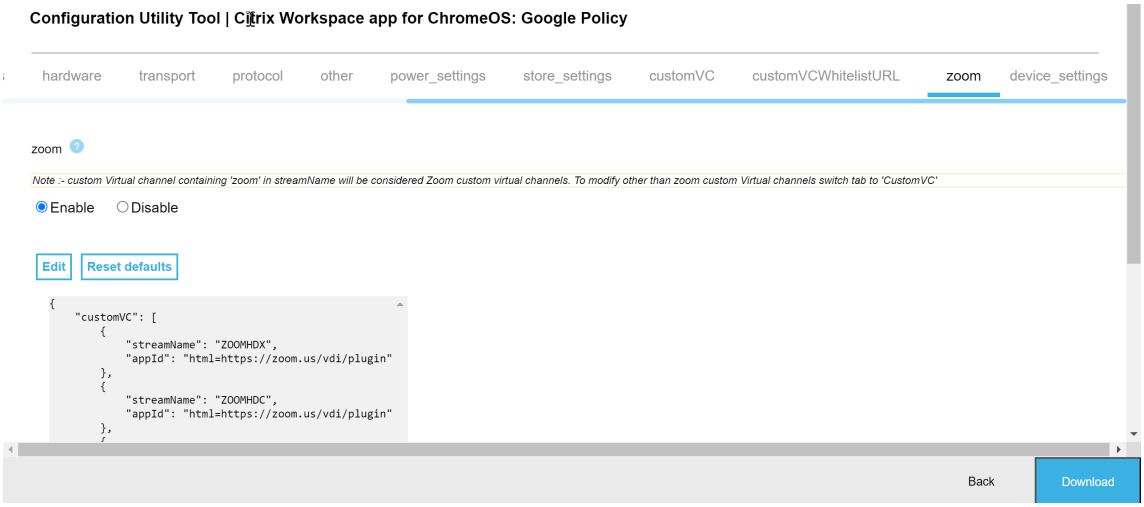
```
27
28 ],
29 "customVCWhitelistURL": [
30    {
31
32        "url": "https://zoom.us/vdi/plugin",
33        "permissions": [
34            "media"
35        ]
36     }
37  ,
38    {
39
40        "url": "https://zoom.us/vdi/webview",
41        "permissions": [
42            "media"
43        ]
44     }
45
46 ]
47  }
48
49  }
50
51  }
52
53 <!--NeedCopy-->
```

4. Guarde los cambios.

Herramienta de la utilidad de configuración

Para personalizar la función:

1. Haga clic en Descargas.
2. Desplácese a la sección de la **herramienta de configuración** y expanda el elemento.
3. Descargue y descomprima el archivo.
4. Haga clic en el enlace a la documentación de la herramienta de configuración para saber cómo usar la herramienta.
5. Cree una configuración de directiva de Google.
6. Desplácese horizontalmente y seleccione la ficha **Zoom**. Habilite la función para continuar.



7. Haga clic en **Descargar** para generar y guardar el archivo **policy.txt**.
8. Personalice esta función según sea necesario proporcionando las URL adecuadas.
9. Abra la aplicación Citrix Workspace en la consola de administración de Google.
10. Cargue el archivo **policy.txt** generado o copie y pegue el contenido.

Configurar la VDI de Zoom para ChromeOS

Para obtener más información, consulte el artículo de asistencia de Zoom Configuring Zoom VDI for ChromeOS.

Varios monitores

May 16, 2024

Presentación en varios monitores

La función de presentación en varios monitores admite hasta dos monitores externos (1 monitor de dispositivo integrado y 2 monitores externos). De manera predeterminada, la función de presentación multimonitor está habilitada.

Los diálogos y barras de herramientas de la interfaz de usuario solo aparecen en el monitor principal. No obstante, los diálogos de tarjeta inteligente y USB abarcan los distintos monitores.

Modo de configuración

De manera predeterminada, la función de presentación multimonitor está habilitada.

> **Nota:**
>
> - Si usa la aplicación Citrix Workspace en XenApp 6.5, configure la directiva de **remedo** como **Inhabilitada** para usar la presentación multimonitor.
> - En una sesión de escritorio, cuando la ventana está en modo de pantalla completa, la opción **Resolución de pantalla** en **Preferencias** está desactivada.
> - Los diálogos y barras de herramientas de la interfaz de usuario solo aparecen en el monitor principal. No obstante, los diálogos de tarjeta inteligente y USB abarcan los distintos monitores.

Para inhabilitar la presentación mejorada en varios monitores en modo quiosco

La presentación mejorada en varios monitores en modo quiosco está habilitada de forma predeterminada.

Para inhabilitar la función en el modo quiosco, modifique el archivo **configuration.js** o la directiva de la **consola de administración de Google** y establezca el valor de **kioskMultimonitor** en **false**.

```
{

    "settings": {

        "Value": {

            "settings_version": "1.0",
            "engine_settings": {

                "features": {

                    "graphics": {

                        "multiMonitor": true,
                        "kioskMultimonitor": true
                    }

                }

            }

        }

    }
```



```
27
28
29 <!--NeedCopy-->
```

> **Nota:**
>
> Para iniciar una sesión en modo quiosco, debe habilitar el modo **Escritorio unificado**.

1. Abra un explorador web e introduzca el comando: chrome://flags
2. En la lista de funciones, busque UnifiedDesktopMode y configúrela como **Habilitada**.

Para configurar el modo Escritorio unificado

1. Inicie una sesión en la Consola de administración de Google.
2. Vaya a **Administración de dispositivos > Administración de Chrome > Configuración de usuario**.
3. Defina la directiva de Google "Escritorio unificado"con el valor **Hacer que el modo Escritorio unificado esté disponible para el usuario**.
4. Haga clic en **Guardar**.

Rendimiento con varios monitores

La aplicación Citrix Workspace para ChromeOS mejora el rendimiento y la estabilidad generales de las sesiones en casos con varios monitores. En versiones anteriores, cuando la sesión disponía de varios monitores, el rendimiento era bajo.

Modo de configuración

Presentación en varios monitores en modo quiosco La presentación mejorada en varios monitores en modo quiosco está habilitada de forma predeterminada.

Para inhabilitar el modo quiosco, modifique el archivo **configuration.js** o la directiva de la **consola de administración de Google** y establezca el valor de **kioskMultimonitor** en **false**.

```
1  {
2
3      "settings": {
4
5          "Value": {
6
7              "settings_version": "1.0",
8              "engine_settings": {
9
10                 "features": {
11
```



```
                    "graphics": {

                        "kioskMultimonitor": false
                    }

                }

            }

        }

    }


<!--NeedCopy-->
```

> **Nota:**
>
> Para iniciar una sesión en modo quiosco, debe habilitar el modo **Escritorio unificado**.

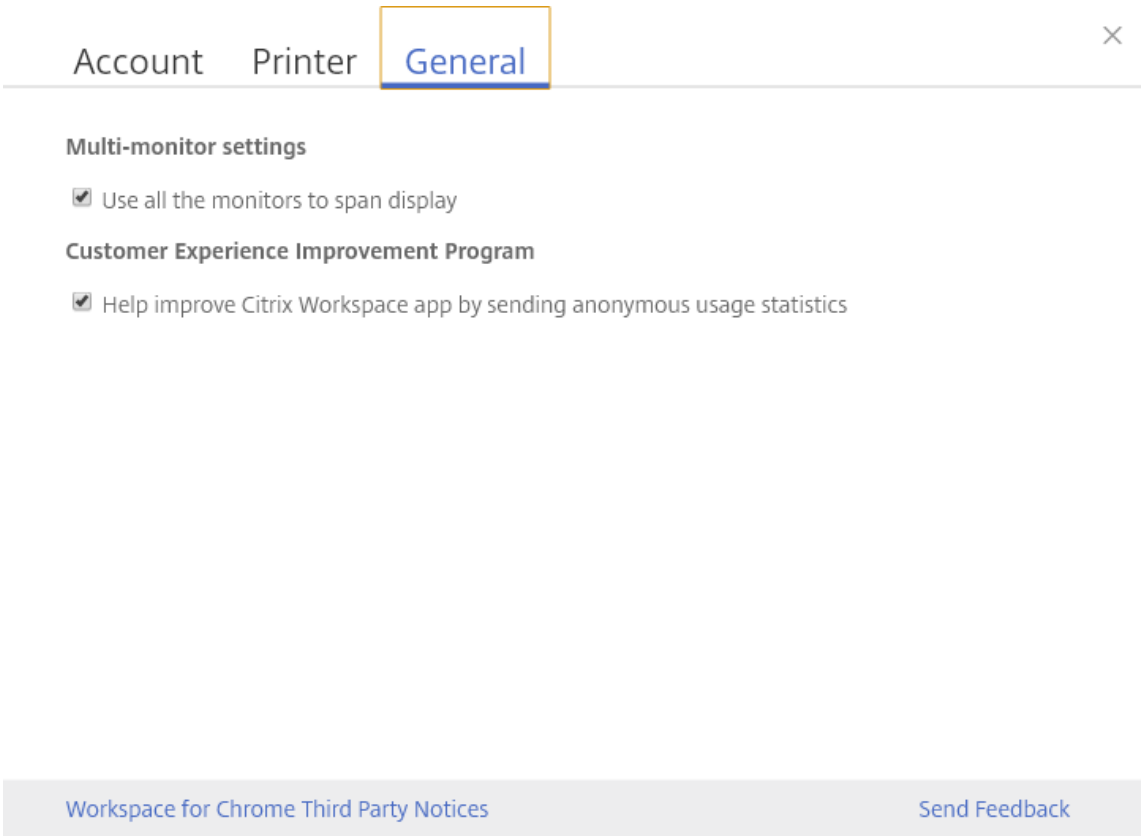
1. Abra un explorador web e introduzca el comando: chrome://flags
2. En la lista de funciones, busque UnifiedDesktopMode y configúrela como **Habilitada**.

Para configurar el modo Escritorio unificado mediante una directiva administrativa de Google

1. Inicie una sesión en la Consola de administración de Google.
2. Vaya a **Administración de dispositivos > Administración de Chrome > Configuración de usuario**.
3. Defina la directiva de Google "Escritorio unificado"con el valor **Hacer que el modo Escritorio unificado esté disponible para el usuario**.
4. Haga clic en **Guardar**.

Para inhabilitar la función de varios monitores De manera predeterminada, la función de presentación multimonitor está habilitada.

1. Inicie la aplicación Citrix Workspace para ChromeOS.
2. Seleccione **Parámetros > General**.
3. Desmarque **Abarcar todos los monitores con la presentación en pantalla**.



La presentación en varios monitores está disponible tanto para escritorios como para aplicaciones.

Al usar la presentación en varios monitores, la sesión de escritorio puede abarcar varios monitores de dos maneras:

4. Modo de ventana: La sesión de escritorio se muestra en modo de monitor único.
5. Modo de pantalla completa: Cuando se cambia la sesión de escritorio al modo de pantalla completa, la sesión se muestra en modo multimonitor solo al seleccionarse **Abarcar todos los monitores con la presentación en pantalla**.

   Para que la pantalla abarque los distintos monitores de una sesión de escritorio, seleccione la opción **Abarcar todos los monitores con la presentación en pantalla** y haga clic en el modo de pantalla completa si ambos monitores están conectados.

   En una sesión de aplicación, cuando hay dos monitores conectados y la opción **Abarcar todos los monitores con la presentación en pantalla** está **habilitada**, la sesión se muestra automáticamente en modo multimonitor.

Usar Citrix Virtual Desktops en monitores dobles:

1. Haga clic en **Multimonitor** en la barra de herramientas.

   La pantalla se extiende ahora a ambos monitores.

Limitaciones de la función:

- La aplicación Citrix Workspace para ChromeOS no admite el modo de gráficos H.264 de pantalla completa para varios monitores.
- El límite de la cantidad de monitores no está codificado de forma rígida. La resolución total que se administrará y representará afecta a estas limitaciones.
  - Esta función admite hasta dos monitores externos (1 monitor de dispositivo integrado y 2 monitores externos). Si inicia una sesión con una resolución de pantalla total superior a [2 x (1920x1080)] píxeles, es posible que sufra demoras en lo que se muestra en pantalla. Los límites en la resolución de monitores pueden provocar retrasos en lo que se muestra en pantalla.
  - La pantalla integrada de los Chromebooks más recientes admite una resolución superior a 1920x1080 píxeles. La función no se ha probado en dichos dispositivos.
- En el modo de varios monitores, H264 en pantalla completa está inhabilitado debido a problemas encontrados durante las pruebas.
  - Cuando se utiliza un solo monitor externo grande, el problema no se produce y H264 no deja de ejecutarse. Selective H264 también se ejecuta en este caso.
- Al usar pantallas con diferentes resoluciones, es posible que experimente problemas de rendimiento.
- Cuando utiliza monitores integrados con una resolución alta y monitores externos cuya resolución es baja, pueden producirse problemas de rendimiento.

Compatibilidad con escritorios virtuales en configuraciones con varios monitores

Ahora puede usar escritorios virtuales en modo de pantalla completa en un subconjunto de monitores disponibles. Antes, al seleccionar el modo multimonitor desde la barra de herramientas, el escritorio virtual abarcaba todos los monitores disponibles. Ahora puede arrastrar su escritorio virtual para que abarque dos monitores (si hay más de dos) y, a continuación, seleccionar el modo multimonitor. Un caso de uso típico es cuando elige ejecutar una aplicación de videoconferencias en el monitor del dispositivo nativo y quiere ver el contenido de su escritorio virtual a pantalla completa en los otros dos monitores durante la llamada.

> **Nota:**
>
> - Para usar esta función, en **Parámetros generales** > **Parámetros multimonitor** > seleccione la opción **Abarcar todos los monitores con la presentación en pantalla**.

Periféricos

May 20, 2024

Redirección de dispositivos USB

La aplicación Citrix Workspace para ChromeOS admite una amplia gama de periféricos USB. Con esta funcionalidad adicional, puede crear una directiva de Google para identificar el PID/VID del dispositivo para habilitar su uso en Citrix Workspace. Esta función también se extiende a nuevos dispositivos USB.

Modo de configuración

Para obtener información sobre la configuración de dispositivos USB, consulte el artículo CTX200825 de Knowledge Center.

Redirección automática de dispositivos USB en modo quiosco

En el modo quiosco, los dispositivos USB se redirigen automáticamente dentro de una sesión sin intervención manual. En los modos público y de usuario, por primera vez, debe redirigir manualmente el dispositivo USB a la sesión desde la barra de herramientas o la Central de conexiones. Esta redirección de USB manual se lleva a cabo para otorgar permiso al sistema operativo Chrome para acceder al dispositivo USB. Cuando se inserta un dispositivo USB, se lo redirige a la sesión automáticamente.

> **Importante:**
>
> - Si inserta un dispositivo USB cuando hay muchas sesiones ejecutándose, el USB se redirige a la sesión activa en ese momento.
> - Si no hay sesiones en foco, el dispositivo USB no se redirige a ninguna sesión.
> - Si hay una sesión activa y no está en el foco al insertar el dispositivo USB, es posible que no tenga lugar la redirección del dispositivo USB.

Para redirigir el dispositivo USB a una nueva sesión

> **Nota:**
>
> Para redirigir el dispositivo USB a una nueva sesión, es necesario quitar el dispositivo USB de la sesión anterior.

1. Haga clic con el botón secundario en el icono de Citrix Workspace y seleccione **Central de conexiones**. Aparece la ventana Central de conexiones.
2. Seleccione una sesión o una aplicación.
3. Haga clic en **Dispositivos**.
4. Vaya a la sección **USB**.
5. Haga clic en **Liberar todo**.

Doble salto

A partir de la versión 2301, la aplicación Citrix Workspace admite casos de doble salto. Esta función es una mejora de la redirección de USB.

Para obtener más información, consulte Doble salto en la documentación de Citrix Virtual Apps and Desktops.

Redirección de dispositivos USB compuestos

Antes, al conectar un dispositivo USB compuesto al dispositivo local, solo se podía usar como un único dispositivo mediante la redirección de USB. La desventaja era que las interfaces como el audio y el vídeo también se redirigían a través de USB, a pesar de los canales optimizados. Las interfaces no se separaban y, debido a esta incapacidad, los administradores no podían decidir qué componentes redirigir a través de USB y cuáles redirigir a través del canal virtual optimizado (como la interfaz de audio) para obtener un rendimiento óptimo.

A partir de la versión 2211, los administradores pueden configurar si ciertas interfaces del dispositivo se redirigen o no a la sesión mediante la redirección de USB. Ahora, el usuario final puede seleccionar y redirigir una interfaz constitutiva específica de un dispositivo USB compuesto a la sesión de la aplicación Citrix Workspace mediante la redirección de USB.

Acerca de la redirección de dispositivos USB compuestos

USB 2.1 y versiones posteriores admiten la noción de dispositivos USB compuestos donde muchos dispositivos secundarios comparten una única conexión con el mismo bus USB. Estos dispositivos emplean un solo espacio de configuración y una conexión de bus compartida, donde se usa un número de interfaz único 00-ff para identificar cada dispositivo secundario. Estos dispositivos no son lo mismo que un concentrador USB que proporciona un nuevo origen de bus USB para otros dispositivos USB con direcciones independientes para la conexión.

Los dispositivos compuestos encontrados en el dispositivo de punto final cliente se pueden reenviar al host virtual como una de estas dos opciones:

- Un solo dispositivo USB compuesto
- Un conjunto de dispositivos secundarios independientes (dispositivos divididos)

Cuando se reenvía un dispositivo USB compuesto, todo el dispositivo deja de estar disponible para el dispositivo local. El reenvío también bloquea el uso local del dispositivo para todas las aplicaciones del dispositivo local, incluida la aplicación Citrix Workspace.

Considere un dispositivo con auriculares USB con un dispositivo de audio y el botón HID para el control de volumen y silencio. Si todo el dispositivo se reenvía mediante un canal USB genérico, el dispositivo deja de estar disponible para la redirección por el canal de audio con HDX optimizado. Sin embargo, puede lograr un mejor rendimiento cuando el audio se envía a través de un canal de audio HDX optimizado en comparación con un canal genérico.

Para resolver estos problemas, Citrix recomienda dividir el dispositivo compuesto y reenviar solo las interfaces secundarias que usan un canal USB genérico. Este mecanismo garantiza que los demás dispositivos secundarios estén disponibles para su uso en las aplicaciones del dispositivo local, incluida la aplicación Citrix Workspace, que ofrece una experiencia con HDX optimizado. Este método permite reenviar los dispositivos necesarios y ponerlos a disposición de la sesión remota.

Cómo habilitar esta función

Puede habilitar esta función de las siguientes maneras:

- Configuration.js
- Global App Configuration Service
- Directiva administrativa de Google

Configuration.js Para configurar la redirección de dispositivos USB compuestos mediante el archivo **configuration.js**, haga lo siguiente:

1. Busque el archivo **configuration.js** en la **carpeta raíz de ChromeApp**.
2. Modifique el archivo **configuration.js** para configurar la función de redirección de dispositivos USB compuestos.

> **Notas:**
>
> - Citrix recomienda hacer una copia de seguridad del archivo **configuration.js** antes de hacer cambios.
> - Citrix recomienda modificar el archivo **configuration.js** solo si la aplicación Citrix Workspace para ChromeOS se reempaqueta para los usuarios.
> - Se requieren credenciales de nivel de administrador para modificar el archivo **configuration.js**.

3. Establezca **enableCompositeDeviceSplit** en **true**.

A continuación se muestra un ejemplo de datos JSON:

```
```
{

    "features": {

        "usb": {

            "enableCompositeDeviceSplit": true
         }

     }

 }

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

1. Guarde los cambios.

> **Nota:**
>
> - Para inhabilitar la función, establezca el atributo **enableCompositeDeviceSplit** en **false**.

**Global App Configuration Service** En la configuración en la nube, los administradores pueden habilitar la función de redirección de dispositivos USB compuestos al establecer el atributo **enableCompositeDeviceSplit** en True en Global App Configuration Service.

Para obtener más información, consulte la documentación de Global App Configuration Service.

**Directiva administrativa de Google** En la implementación local, los administradores pueden habilitar la función de redirección de dispositivos USB compuestos mediante la directiva administrativa de Google de la siguiente manera:

1. Inicie sesión en la directiva administrativa de Google.
2. Vaya a **Administración de dispositivos** > **Administración de Chrome** > **Configuración de usuario**.
3. Agregue estas cadenas al archivo **policy.txt** en la clave engine_settings. A continuación se muestra un ejemplo de datos JSON:

```
{

    "features": {

        "usb": {
```


```

```
6
7   "enableCompositeDeviceSplit": true
8   }
9
10   }
11
12   }
13
14 <!--NeedCopy-->
```

4. Guarde los cambios.

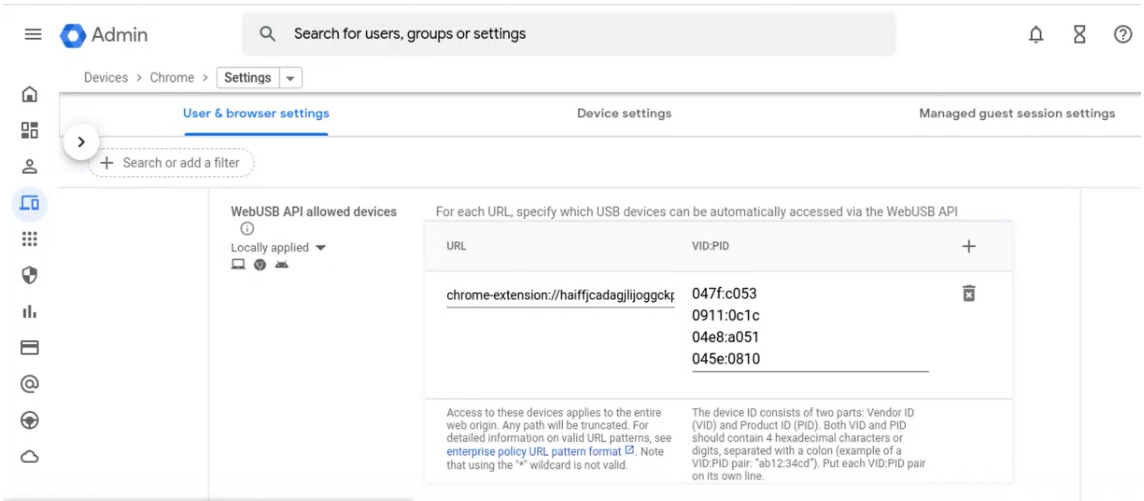
Configuración

Requisitos previos:

- Incluya la lista de dispositivos USB permitidos con valores VID:PID y habilite la directiva de redirección de dispositivos USB en Delivery Controller. Para obtener más información, consulte el artículo CTX200825 de Knowledge Center.
- Esta función funciona en dispositivos administrados, pero no en dispositivos BYOD.

Para habilitar la detección automática de USB:

1. Vaya a la configuración de la directiva administrativa de Google.
2. Seleccione la opción **WebUSB API allowed devices**.
3. Introduzca la aplicación Citrix Workspace para el ID de extensión de ChromeOS. Por ejemplo, chrome-extension: `//haiffjcadagjlijoggckpgfnoeiflnem`.
4. Agregue el VID y el PID del dispositivo de la siguiente manera:



Ahora, tras agregar los valores de VID y PID, la aplicación Citrix Workspace puede detectar automáticamente los dispositivos de la sesión.

5. Aplique la directiva administrativa de Google. Para obtener más información sobre las reglas del dispositivo y los datos JSON de muestra, consulte la siguiente sección.
6. Guarde los cambios.

Reglas de dispositivo

La aplicación Citrix Workspace usa las reglas del dispositivo para decidir a qué dispositivos USB se les permite o se les impide el reenvío a la sesión remota.

A continuación se explican las palabras clave:

- **allow:** Esta sección incluye la lista de dispositivos y las interfaces secundarias que se pueden redirigir a la sesión.
- **deny:** Esta sección incluye la lista de dispositivos y las interfaces secundarias que no se pueden redirigir a la sesión.
- **autoRedirect:** Esta sección incluye la lista de dispositivos y las interfaces secundarias que se pueden redirigir automáticamente a la sesión mediante la redirección de USB.

  > **Nota:**
  >
  > - Cada objeto representa un dispositivo con los valores obligatorios `vid` y `pid` del dispositivo USB. Es opcional incluir los valores "split"e "interfaceClass".

- **vid, pid (obligatorio):** Representa el ID de proveedor (VID) y el ID de producto (PID) del dispositivo USB. Introduzca los valores en formato hexadecimal.
- **split (opcional):** Espera un valor booleano que indica si el dispositivo se divide en interfaces secundarias o no.
- **interfaceClass (opcional):** Representa la clase de interfaz del USB. Los valores permitidos son audio, video, hid, printer, storage…

A continuación se muestra un ejemplo de datos JSON:

```
{

"settings": {

"value": {

"settings_version": "1.0",
"device_settings": {

"deviceRules": {


```



```
    "allow": [
        {
"vid": "11","pid": "22",  "split":true, "interfaceClass":["audio","
    video"] }
 //split device and allow redirection of 'audio' & 'video' interfaces.
    ],

    "deny": [
        {
"vid": "33","pid": "44" }
,  //deny redirection of this whole device with vid= 33 & pid = 44,
    including all of its interfaces.
        {
"vid": "77","pid": "88","split":true,"interfaceClass":["audio"] }
     //split device and deny the redirection of 'audio' interface only;
          remaining interfaces(if any) are redirected through USB.
    ],

    "autoRedirect": [
    {
"vid": "55","pid": "66" }
, //auto redirect the device when it's connected.
    {
"vid": "55","pid": "66","split":true,"interfaceClass":["hid"] }
 //split device and auto redirect only the 'hid' interface when the
     device is connected.
    ]
                }

            }

        }

     }

 }

<!--NeedCopy-->
```

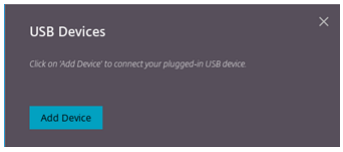
Cómo utilizar esta función

Para utilizar la función de redirección de dispositivos USB compuestos:

1. Haga clic en el icono de USB de la barra de herramientas.

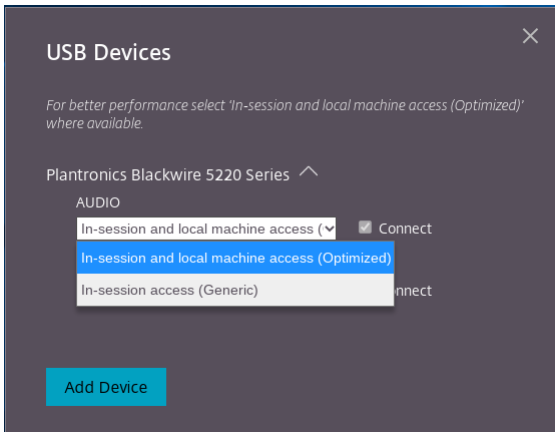
   

   Si no hay ningún dispositivo USB conectado, aparece esta ventana emergente:

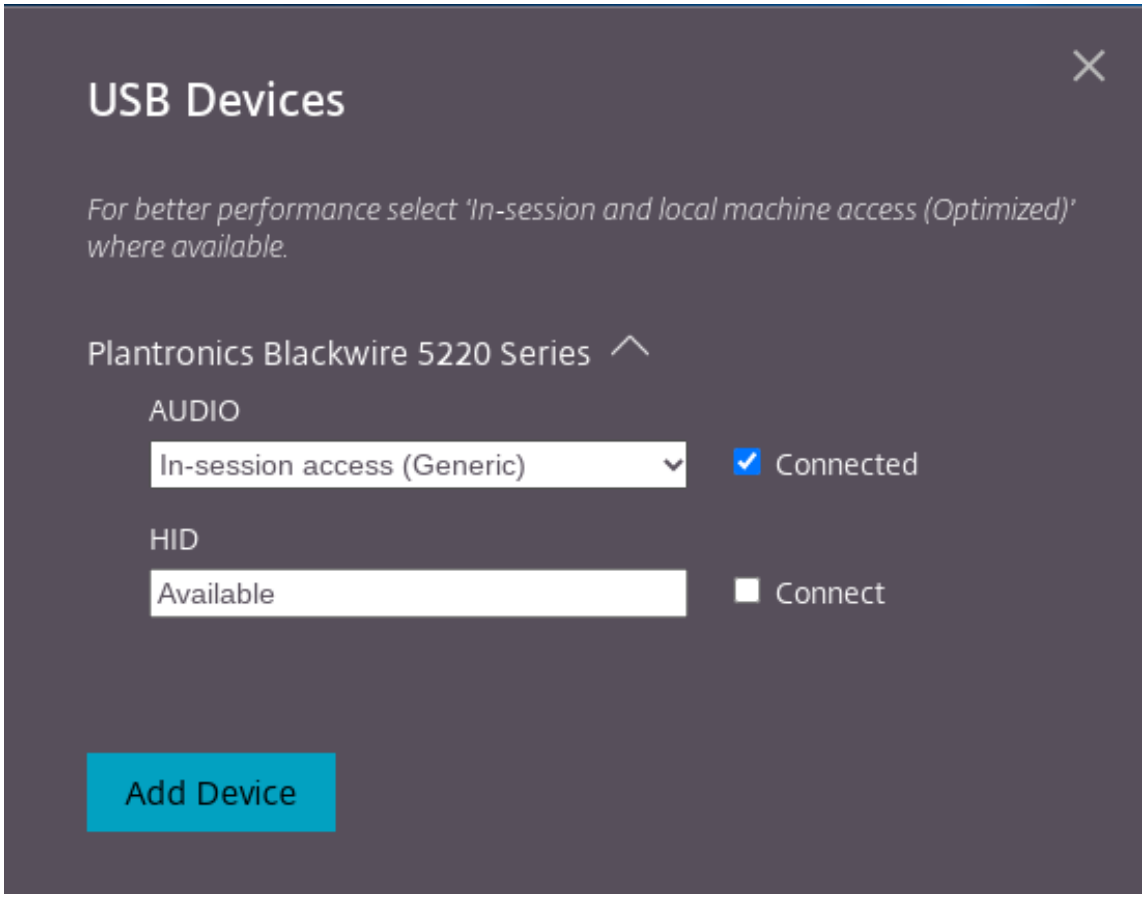


2. Conecte un dispositivo USB a la máquina local.
   Es posible que aparezca esta ventana emergente:
3. Haga clic en **Dispositivos USB** para ver y redirigir la interfaz constituyente del USB. Tras una conexión correcta, la aplicación Citrix Workspace detecta el USB. Para cada interfaz constituyente del USB, verá un menú desplegable. Las dos opciones son:

   - **Acceso en sesión y a la máquina local (optimizado):** Seleccione esta opción si quiere acceder al USB en su dispositivo y en una sesión.
   - **Acceso en sesión (genérico):** Seleccione esta opción si quiere acceder al USB solo en la sesión.
     Para obtener un mejor rendimiento, seleccione la opción **Acceso en sesión y a la máquina local (optimizado)**.



4. Seleccione **Conectar** para redirigir la interfaz.



Si la redirección se realiza correctamente, el estado cambia a **Conectado**.

> **Notas:**
>
> - Para agregar un dispositivo USB de forma manual, haga clic en **Agregar dispositivo**. Aparecerá el cuadro de diálogo del selector de Chrome con una lista de los dispositivos USB. Puede seleccionar el dispositivo de la lista.
> - Si se deniega la conexión de un dispositivo USB, aparecerá este mensaje de error:
>
> "El administrador bloqueó el dispositivo recién insertado.
> Contacte con el administrador de su organización para obtener asistencia.

Cómo transferir la interfaz del USB entre las sesiones

Al hacer clic en el icono de USB de la barra de herramientas, aparece una lista de los dispositivos USB que están conectados a las sesiones. Si el dispositivo USB ya se está usando en otra sesión, puede ver que la interfaz constituyente del USB muestra el estado **Conectado a otra sesión**.

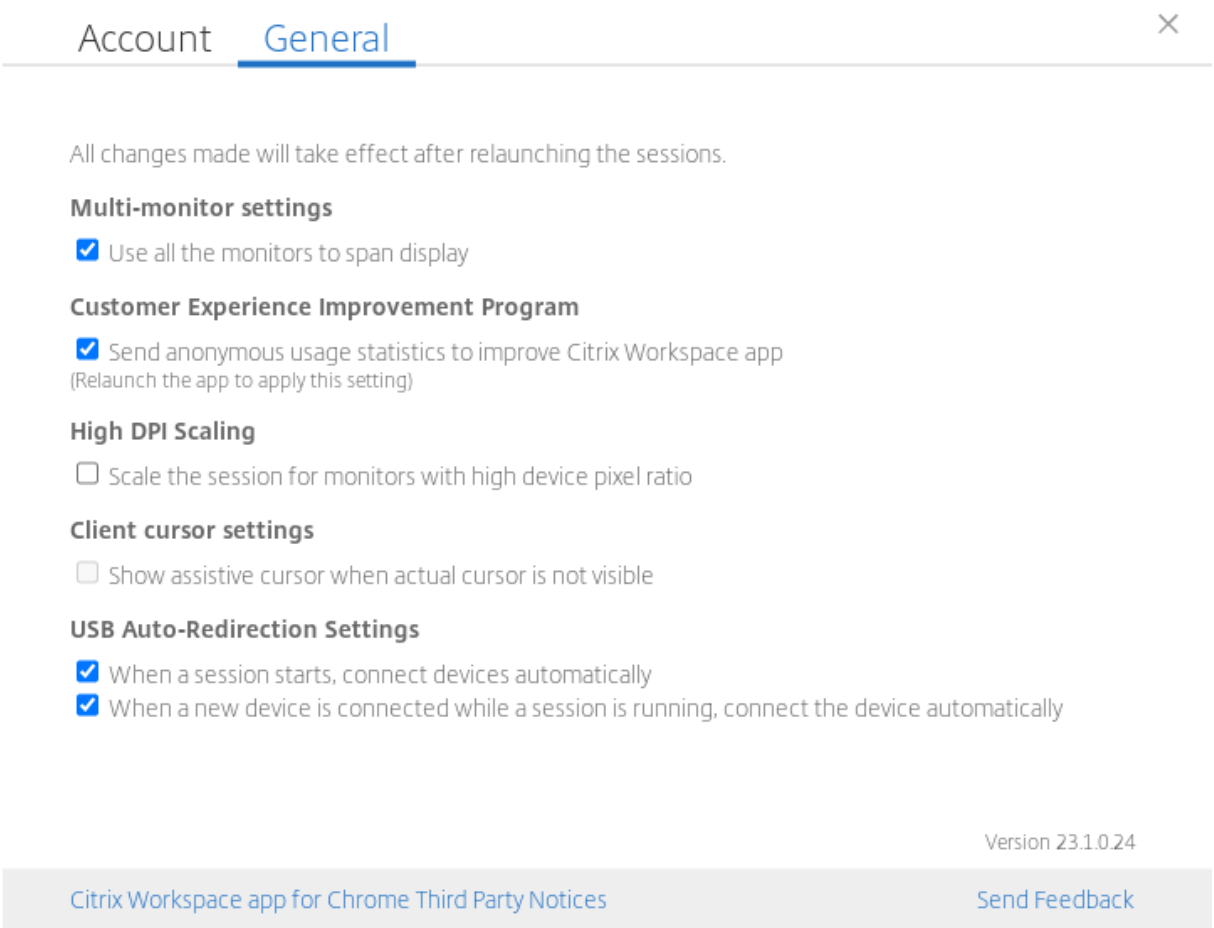
Para redirigirlo a la sesión actual, seleccione **Conectado**, que se encuentra al otro lado de la interfaz constituyente del USB. El estado cambia en consecuencia.

Parámetros de redirección automática de USB compuestos

Antes, no había ninguna opción relacionada con los parámetros de redirección automática de USB para configurar las preferencias del usuario final. Como los administradores controlan estas directivas, el usuario final tiene que redirigir manualmente los dispositivos USB necesarios en el inicio de cada sesión.

A partir de la versión 2301, el usuario final puede seleccionar una preferencia de redirección automática para cualquier dispositivo USB dentro de una sesión de Virtual Desktops. Ahora, la aplicación Citrix Workspace proporciona parámetros al nivel de la aplicación, donde el usuario final puede controlar la redirección automática de USB. El usuario final puede establecer sus preferencias y guardar los parámetros para los siguientes inicios de sesión.

Hay dos opciones: una al iniciar las sesiones y otra mientras la sesión está en curso.



Nota:

- Esta función admite implementaciones locales y en la nube, y solo está disponible para usuarios de Chrome administrados.

Configurar la redirección de dispositivos USB compuestos mediante directivas de DDC

Antes, los administradores usaban directivas de administración de Google para configurar la redirección de USB del lado del cliente.

A partir de la versión 2306, también puede configurar la redirección de USB mediante las directivas de DDC. Las configuraciones mediante directivas de DDC permiten que los administradores dispongan de una forma unificada y centralizada de definir directivas y comportamientos. Estas directivas se aplican a implementaciones locales y de la nube en dispositivos y usuarios administrados. Esta función está disponible en VDA 2212 y versiones posteriores.

Configuración

Puede configurar esta función de una de estas maneras:

- Configuration.js
- Directiva administrativa de Google

> **Nota:**
>
> - La directiva **enableDDCUSBPolicy** se establece en **true** de forma predeterminada.

Configuration.js Para inhabilitar esta función mediante el archivo **configuration.js**, haga lo siguiente:

1. Busque el archivo **configuration.js** en la carpeta **raíz de ChromeApp**.
2. Modifique el archivo.

   > **Notas:**
   >
   > - Citrix recomienda hacer una copia de seguridad del archivo **configuration.js** antes de hacer cambios.
   > - Citrix recomienda modificar el archivo **configuration.js** solo si la aplicación Citrix Workspace para ChromeOS se reempaqueta para los usuarios.
   > - Se requieren credenciales de nivel de administrador para modificar el archivo **configuration.js**.

3. Establezca el valor de **enableDDCUSBPolicy** en **false**. A continuación se muestra un ejemplo de datos JSON:

```
"features" : {

"usb" : {

```



```
    "enableDDCUSBPolicy": false
      }

 }

<!--NeedCopy-->
```

4. Guarde los cambios.

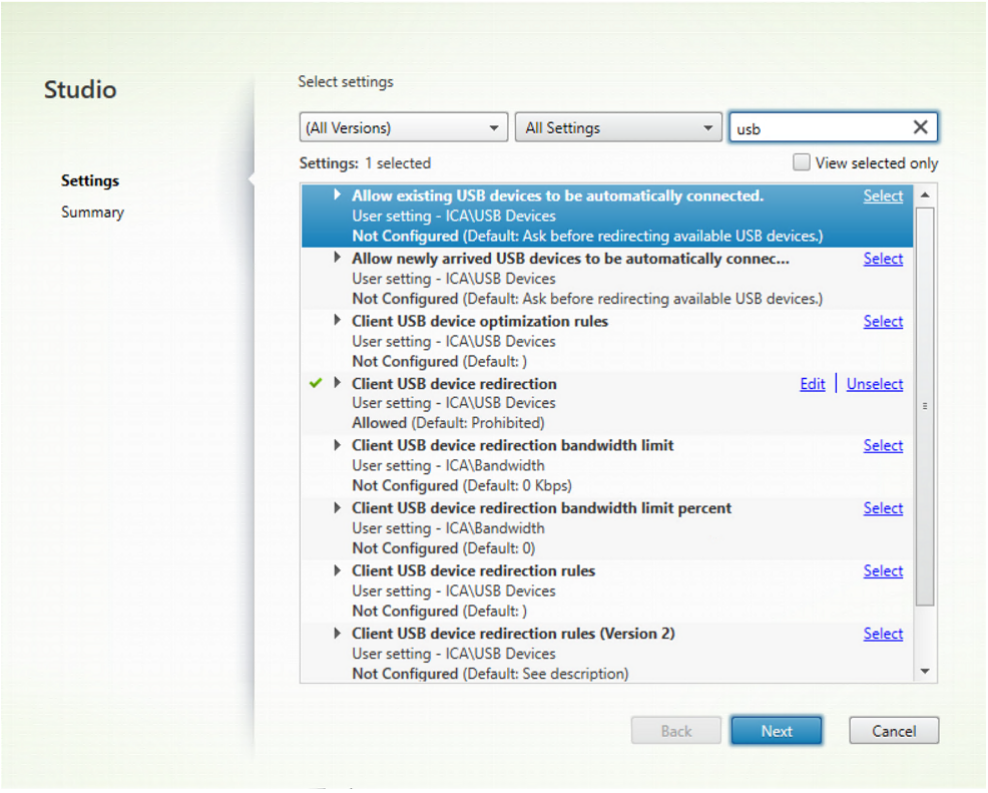
Directiva administrativa de Google Para los usuarios y dispositivos administrados, los administradores pueden inhabilitar esta función mediante la directiva administrativa de Google de esta manera:

1. Inicie sesión en la directiva administrativa de Google.
2. Vaya a **Administración de dispositivos** > **Administración de Chrome** > **Configuración de usuario**.
3. Agregue estas cadenas al archivo **policy.txt** en la clave engine_settings.
   A continuación se muestra un ejemplo de datos JSON:

```
    "features" : {

    "usb" : {

       "enableDDCUSBPolicy": false
     }

 }

<!--NeedCopy-->
```

4. Guarde los cambios.

Directiva de DDC Esta captura de pantalla muestra las directivas de DDC relacionadas con la redirección de USB. Esta función está disponible en VDA 2212 y versiones posteriores.



Para obtener más información sobre las directivas de DDC relacionadas con la redirección de USB, consulte estos artículos de la documentación de Citrix Virtual Apps and Desktops:

- Reglas de redirección de dispositivos USB del cliente
- Permitir que los dispositivos USB existentes se conecten automáticamente.
- Permitir que los dispositivos USB recién llegados se conecten automáticamente.
- Reglas de redirección de dispositivos USB del cliente (versión 2).

Redirección automática de dispositivos USB

Para redirigir dispositivos USB automáticamente, debe seguir las reglas de los dispositivos USB. Puede configurar las reglas de los dispositivos USB mediante:

- Directiva administrativa de Google
- Reglas de redirección de dispositivos USB del cliente (versión 2)

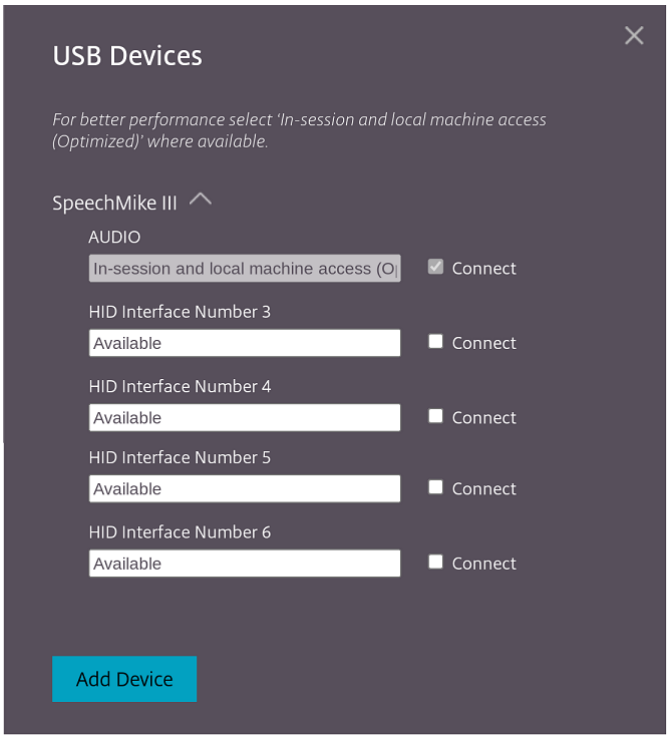
Mejoras en la interfaz de usuario de dispositivos USB compuestos

A partir de la versión 2306, cuando la configuración de un dispositivo USB compuesto está definida en "split": true, la interfaz de usuario de **Dispositivos USB** muestra los componentes en función de números de la interfaz en lugar de clases de la interfaz.

Para obtener más información, consulte el artículo Redirección de dispositivos USB compuestos.

Interfaz de usuario

A continuación, se muestra un ejemplo:



Mejoras en la redirección de dispositivos USB compuestos mediante directivas de DDC

A partir de la versión 2307, puede determinar si una clase o interfaz de USB compuesto concreto puede redirigir al VDA de forma predeterminada o no. Si tiene un USB compuesto conectado al dispositivo ChromeOS, la configuración **enableDefaultAllowPolicy** le ayuda a decidir si, de forma predeterminada, puede permitir la redirección de USB mediante directivas de DDC. La versión 2212 de VDA y las posteriores ofrecen esta función.

Cómo utilizarlo

Al definir el atributo **enableDefaultAllowPolicy** en **true** y redirigir una clase o número de interfaz en particular al VDA, debe agregar una regla de directiva para impedir que se redirijan las demás clases o números de interfaz. Puede configurar esta función mediante la directiva de DDC **Reglas de redirección de dispositivos USB del cliente (versión 2)**.

Para obtener más información, consulte Reglas de redirección de dispositivos USB (versión 2). Además, puede configurar la parte de denegación a través de la directiva administrativa de Google, pero solo para el nivel de clase de la interfaz.

Para obtener más información, consulte Mejoras en la interfaz de usuario de dispositivos USB compuestos.

A continuación se muestra un ejemplo de configuración mediante la directiva de DDC **Reglas de redirección de dispositivos USB del cliente (versión 2)**, en la que se permite la redirección de la interfaz número 03.

```
1 ```
2 "DENY: vid=1188 pid=A301 split=01 intf=00,01,02"
3 <!--NeedCopy--> ```
```

A continuación se muestra un ejemplo de configuración mediante la regla de la directiva administrativa de Google, en la que se permite que la interfaz de HID redirija y deniegue la clase de la interfaz de audio.

```
1 ```
2 "deny": [
3     {
4  "vid":"05e9", "pid":"0428", "split":true, "interfaceClass":["audio"]
5      }
6
7 ]
8 <!--NeedCopy--> ```
```

Configuración Puede configurar esta función de una de estas maneras:

- Configuration.js
- Directiva administrativa de Google

> **Nota:**
>
> - De forma predeterminada, la directiva **enableDefaultAllowPolicy** está establecida en **true**.

Configuration.js Para inhabilitar esta función mediante el archivo **configuration.js**, haga lo siguiente:

1. Busque el archivo **configuration.js** en la carpeta **raíz de ChromeApp**.
2. Modifique el archivo.

> **Notas:**
>
> - Citrix recomienda hacer una copia de seguridad del archivo **configuration.js** antes de hacer cambios.
> - Citrix recomienda modificar el archivo **configuration.js** solo si la aplicación Citrix Workspace para ChromeOS se reempaqueta para los usuarios.
> - Se requieren credenciales de nivel de administrador para modificar el archivo **configuration.js**.

3. Establezca el valor de **enableDefaultAllowPolicy** en **false**.

   A continuación se muestra un ejemplo de datos JSON:

```
"features" : {

   "usb" : {

   "enableDefaultAllowPolicy": false
     }

 }

<!--NeedCopy-->
```

4. Guarde los cambios.

Directiva administrativa de Google Para los usuarios y dispositivos administrados, los administradores pueden inhabilitar esta función mediante la directiva administrativa de Google de esta manera:

1. Inicie sesión en la directiva administrativa de Google.
2. Vaya a **Administración de dispositivos** > **Administración de Chrome** > **Configuración de usuario**.
3. Agregue estas cadenas al archivo **policy.txt** en la clave **engine_settings**.

   A continuación se muestra un ejemplo de datos JSON:

```
'features' : {

    'usb' : {

    'enableDefaultAllowPolicy': {
 "type": "false" }

     }

   }
```



```
11
12  <!--NeedCopy-->
```

4. Guarde los cambios.

Redirección de puertos COM serie

De manera predeterminada, la aplicación Citrix Workspace para ChromeOS asigna COM5 como puerto COM serie preferido para la redirección.

Modo de configuración

Para configurar la redirección de puertos COM serie, habilite la función aplicando configuraciones de directiva de redirección de puertos de Citrix Virtual Apps and Desktops y Citrix DaaS. Para obtener más información sobre la redirección de puertos, consulte Configuraciones de directiva de Redirección de puertos.

> **Nota:**
>
> De manera predeterminada, la aplicación Citrix Workspace para ChromeOS asigna COM5 como puerto COM serie preferido para la redirección.

Después de habilitar las configuraciones de directiva de redirección de puertos COM serie en el VDA, configure la aplicación Citrix Workspace para ChromeOS mediante uno de estos métodos:

- Directiva administrativa de Google
- Archivo configuration.js
- Cambiando la asignación predeterminada emitiendo un comando en una sesión ICA activa.

Uso de la directiva administrativa de Google para configurar la redirección de puertos COM
Modifique el archivo de directivas para usar este método con el que redirigir el puerto COM serie.

> **Sugerencia:**
>
> Citrix recomienda configurar el puerto COM mediante el archivo de directivas solo cuando la aplicación Citrix Workspace para ChromeOS se reempaquete.

Modifique la directiva administrativa de Google para incluir lo siguiente:

```
1     {
2
3       "settings": {
4
5               "Value": {
```



```
6
7                   "settings_version": "1.0",
8                   "store_settings": {
9
10                  "rf_web": {
11
12                  "url": "<http://YourStoreWebURL>"
13                    }
14
15                    }
16  ,
17                   "engine_settings":{
18
19                   "features" : {
20
21                   "com" : {
22
23          "portname" : "<COM4>", where COM4 indicates the port number that
             is set by the administrator.
                                                  }
24
25                                             }
26
27                                             }
28
29                                             }
30
31                                             }
32
33                                            }
34
35
36  <!--NeedCopy-->
```

Lista de opciones de nombre de puerto COM serie, junto con sus descripciones:

- “portname”: Número de puerto para el canal virtual COM (serie). De forma predeterminada, el valor es COM5.

Uso del archivo configuration.js para configurar la redirección de puertos COM Use este método para redirigir el puerto COM serie con la modificación del archivo **configuration.js**. Busque el campo “portname”en el archivo configuration.js y modifique el valor cambiando el número de puerto.

Por ejemplo:

```
1  "com" :{
2
3
4  "portname" : "COM4"
5
6   }
```



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

> **Nota:**
>
> Citrix recomienda usar el método del archivo configuration.js para configurar la redirección de puertos solo cuando la aplicación Citrix Workspace para ChromeOS se reempaquete y se publique de nuevo desde StoreFront.

Emisión de un comando en una sesión ICA para configurar la redirección de puertos COM Utilice este método para redirigir el puerto COM serie. Ejecute este comando en una sesión ICA activa:

```
1     net use COM4 : \Client\COM5
2 <!--NeedCopy-->
```

> **Sugerencia:**
>
> En el ejemplo de arriba, COM4 es el puerto serie preferido para la redirección.

Parámetros de alimentación

May 16, 2024

Configurar el parámetro Permanecer activado

La aplicación Citrix Workspace para ChromeOS mantiene activos los dispositivos administrados Chromebook incluso cuando los usuarios no están activos.

La función de permanecer activado está inhabilitada de forma predeterminada.

Modo de configuración

Para habilitar la función, modifique la directiva de la **consola de administración de Google** y establezca el valor de propiedad de **keep_awake_level**(mantener activado) de **power_settings** en **"system"** o en **"display"** y luego reinicie sesión.

El nivel **"sistema"** mantiene el sistema activo, pero permite oscurecer o apagar la pantalla. El nivel **"pantalla"** mantiene el sistema activado.

```
1 {
2
```



```
 "settings": {

     "Value": {

         "settings_version": "1.0",
         "power_settings": {

             "keep_awake_level":  ” system ”  or  “ display ”
              }

            }

         }

     }

<!--NeedCopy-->
```

Lista de opciones de configuración de energía, junto con sus descripciones:

- “keep_awake_level”: Mantiene los dispositivos activados, incluso cuando los usuarios no están activos. Puede elegir uno de los dos valores:
  - “system”: Mantiene el sistema activado, pero permite oscurecer o apagar la pantalla.
  - “display”: Mantiene el sistema activado.

> **Nota:**
>
> En el modo quiosco, asegúrese de que la opción **Allow app to manage power** (Permitir que la aplicación administre la energía) en la consola de administración de **Google** esté inhabilitada.

Impresión

May 16, 2024

Impresión de PDF

El controlador Citrix PDF Universal Printer permite a los usuarios imprimir documentos abiertos con aplicaciones alojadas o aplicaciones ejecutadas en escritorios virtuales entregados por XenDesktop 7.6 y XenApp 7.6. Cuando un usuario selecciona la opción Citrix PDF Printer, el controlador convierte el archivo en PDF y lo transfiere al dispositivo local. El PDF se abre en una ventana nueva para verlo e imprimirlo.

Al imprimir un documento abierto con una aplicación alojada o una aplicación que se ejecuta en un escritorio virtual, puede imprimir el documento en PDF. Puede transferir el PDF al dispositivo local

para verlo e imprimirlo desde una impresora conectada localmente. El archivo no se almacena en la aplicación Citrix Workspace para ChromeOS.

> **Importante**
>
> La impresión local en PDF solo se ofrece en XenApp y XenDesktop 7.6 o versiones posteriores.

Modo de configuración

Requisitos Para acceder a la página de descarga de la aplicación Citrix Workspace para ChromeOS, necesita una cuenta de MyCitrix.

Para que los usuarios puedan imprimir documentos abiertos con escritorios y aplicaciones alojadas:

1. Descargue la impresora Citrix PDF Printer e instale el controlador Citrix PDF Universal Printer en cada máquina VDA que entregue escritorios o aplicaciones a usuarios de la aplicación Citrix Workspace. Después de instalar el controlador de la impresora, reinicie la máquina.
2. En Citrix Studio, seleccione el **nodo Directiva** del panel de la izquierda y cree una directiva o modifique una directiva existente.

   Para obtener más información sobre la configuración de directivas de Citrix Virtual Apps and Desktops, consulte las Directivas.
3. Establezca la configuración de directiva Crear automáticamente la impresora universal de PDF en **Habilitada**.

Compatibilidad con impresoras de red

Anteriormente, la opción Citrix PDF Printer se utilizaba para imprimir desde la sesión de escritorio virtual. El controlador de impresión convertía el archivo a formato PDF y lo transfería al dispositivo local. El PDF se abría en una ventana nueva para verlo e imprimirlo.

A partir de la versión 2305, la aplicación Citrix Workspace para ChromeOS admite la impresión en red. Los usuarios finales pueden ver la lista de impresoras que están conectadas a su Chromebook dentro de la sesión. Los usuarios pueden seleccionar una impresora directamente sin generar archivos PDF intermedios en el dispositivo local. Esta función se admite en:

- VDA 2112 y versiones posteriores.
- ChromeOS 112 y versiones posteriores.

> **Nota:**
>
> - De forma predeterminada, esta función está habilitada y solo se admite el formato PDF de

> impresión de metarchivos.

Para obtener información, consulte estos artículos:

- Administrar impresoras y controladores de impresión en su entorno en la documentación de Citrix Virtual Apps and Desktops.
- Artículo de Knowledge Center sobre cómo utilizar la directiva de Citrix para configurar una impresora de sesión predeterminada: CTX232031.
- Artículo de Knowledge Center sobre la guía de inicio rápido de Impresión de Citrix y la configuración predeterminada: CTX227534.

Configuración

Puede inhabilitar esta función de una de estas maneras:

- Configuration.js
- Directiva administrativa de Google

> **Nota:**
>
> - Como requisito previo, el administrador de TI debe habilitar la directiva **Crear automáticamente una impresora universal genérica** en el Delivery Controller (DDC). Para obtener más información, consulte Configuraciones de directiva de Impresoras del cliente en la documentación de Citrix Virtual Apps and Desktops.

Configuration.js Para inhabilitar esta función mediante el archivo **configuration.js**, haga lo siguiente:

1. Busque el archivo **configuration.js** en la carpeta raíz de ChromeApp.

   > **Notas:**
   >
   > - Citrix recomienda hacer una copia de seguridad del archivo **configuration.js** antes de hacer cambios.
   > - Citrix recomienda modificar el archivo **configuration.js** solo si la aplicación Citrix Workspace para ChromeOS se reempaqueta para los usuarios.
   > - Se requieren credenciales de nivel de administrador para modificar el archivo **configuration.js**.

2. Modifique el archivo **configuration.js** y establezca el valor predeterminado de **networkPrinting** en false. A continuación se muestra un ejemplo de datos JSON:


```
{

  "features": {

     " networkPrinting ": {

          "enable": false
                      }

     }

 }

<!--NeedCopy-->
```

3. Guarde los cambios.

Directiva administrativa de Google Los administradores de TI pueden inhabilitar esta función mediante la directiva administrativa de Google de la siguiente manera:

1. Inicie sesión en la directiva administrativa de Google.
2. Vaya a **Administración de dispositivos** > **Administración de Chrome** > **Configuración de usuario**.
3. Agregue estas cadenas al archivo **policy.txt** en la clave **engine_settings**. A continuación se muestra un ejemplo de datos JSON:

```
{

   "features": {

        " networkPrinting ": {

            "enable": false
                 }

         }

 }

<!--NeedCopy-->
```

4. Guarde los cambios.

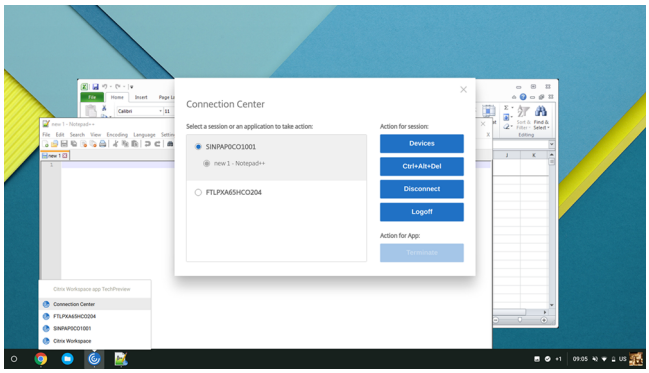
Experiencia nativa

May 16, 2024

Central de conexiones

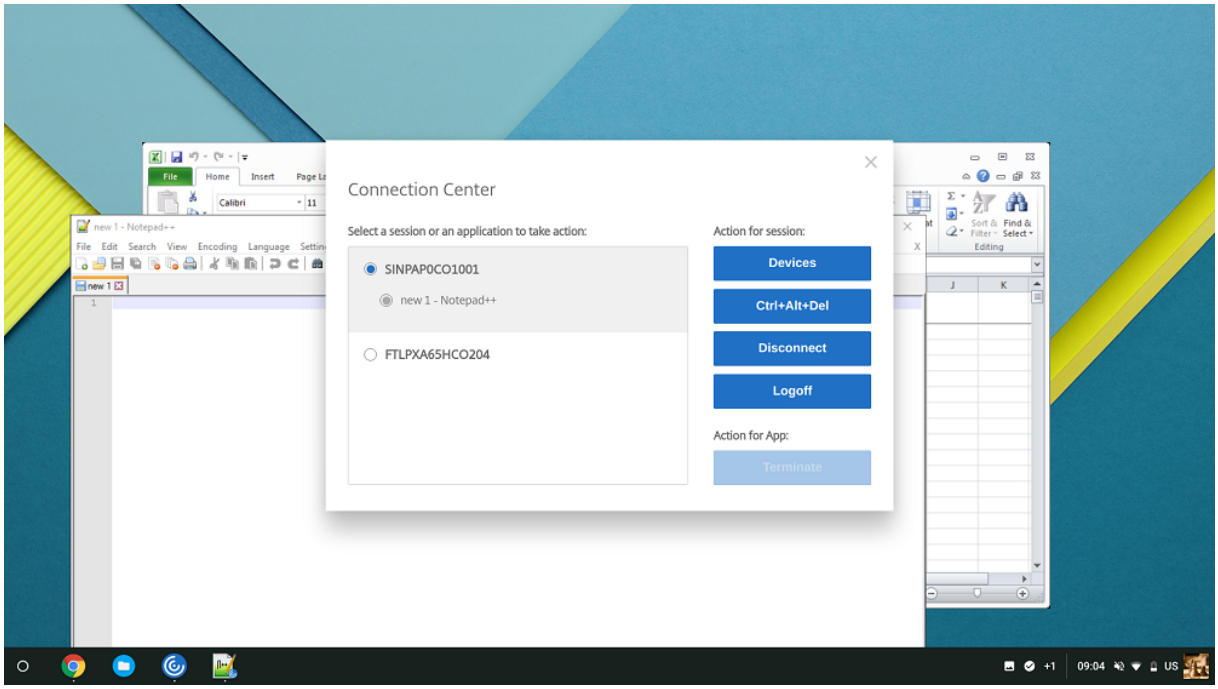
La Central de conexiones ayuda a administrar las aplicaciones en sesiones integradas, presentando una barra de tareas que enumera todas las aplicaciones que están abiertas.

Para abrir la Central de conexiones, haga clic con el botón secundario en el icono de la aplicación Citrix Workspace y haga clic en **Central de conexiones**.



Con la Central de conexiones, puede elegir una aplicación y:

1. Mostrar dispositivos.
2. Enviar comandos Ctrl+Alt+Supr.
3. Desconectarse de una sesión.
4. Cerrar la sesión.

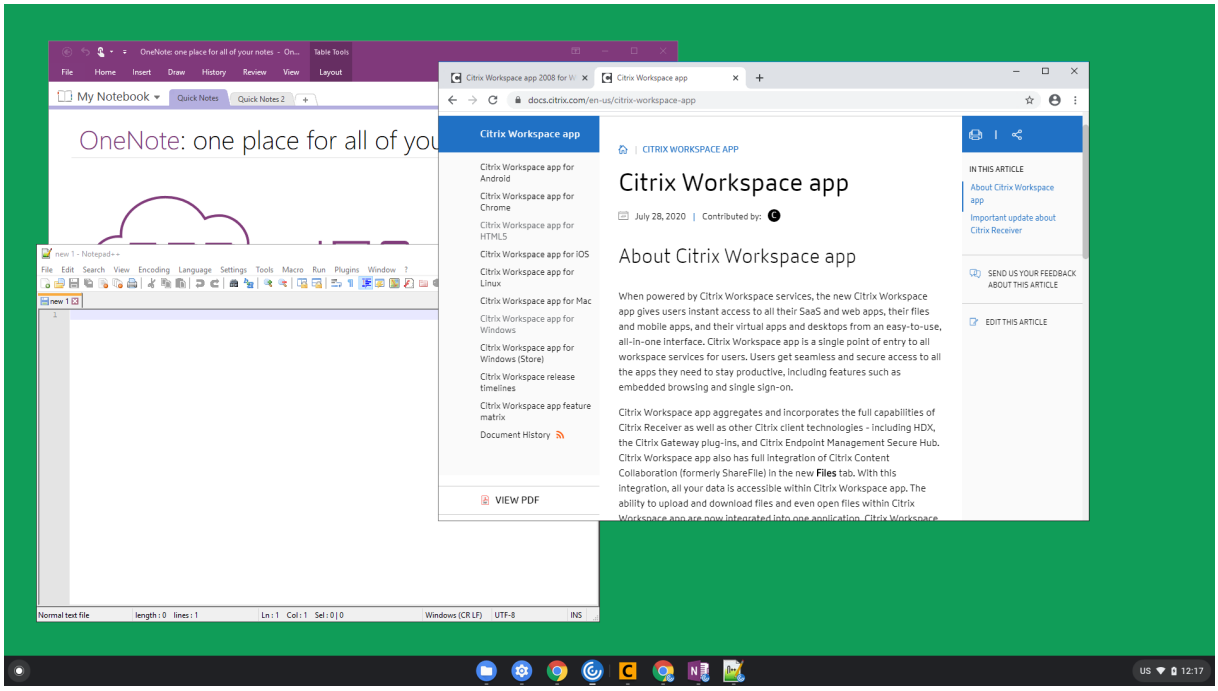


También puede finalizar una aplicación desde la Central de conexiones seleccionando el botón de opción de la aplicación correspondiente y haciendo clic en **Finalizar**.

Ventanas integradas

La aplicación Citrix Workspace para ChromeOS mejora la experiencia del usuario al permitir la integración sin fisuras de varias aplicaciones que están alojadas en ventanas distintas dentro de una sesión activa. Con esta función, la aplicación Citrix Workspace para ChromeOS le permite iniciar aplicaciones en una interfaz de usuario independiente en lugar de iniciar todas las aplicaciones de una sesión en una misma ventana.

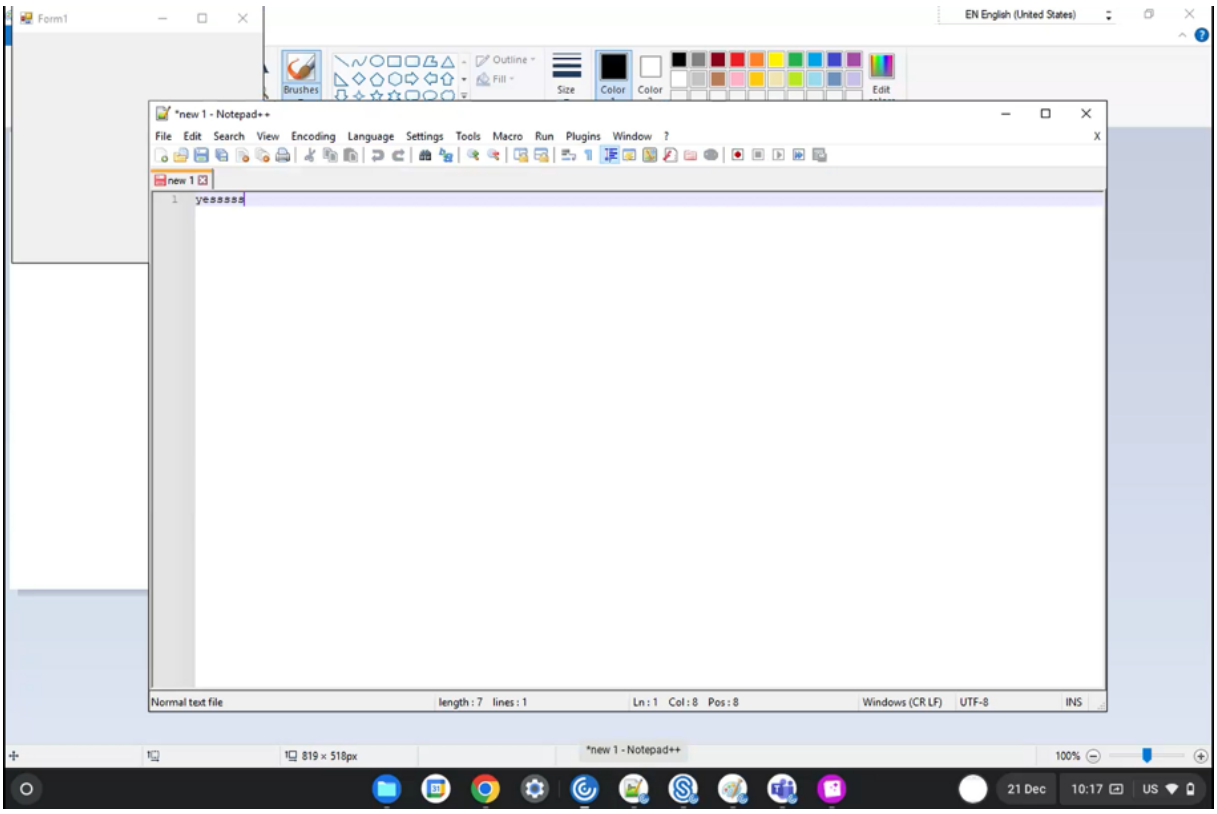
Las aplicaciones integradas se pueden alojar en ventanas separadas. Con esta funcionalidad, las aplicaciones remotas se ejecutan de forma nativa en el dispositivo cliente.



Limitaciones de la función:

- Las entradas adicionales aparecen en la barra de tareas de Chrome. Haga clic en cualquiera de estas entradas para poner la sesión seleccionada al frente.
- Todas las aplicaciones abiertas en una sesión activa se ejecutan en una sola ventana. Al poner el foco en una sesión activa, se lleva el foco a esa ventana junto con todas las aplicaciones que pertenezcan a esa sesión.

Use el icono de aplicaciones integradas de la barra de tareas de la sesión integrada para moverse rápidamente entre las aplicaciones:



> **Sugerencia:**
>
> Todas las aplicaciones de una sesión se ejecutan en una ventana única. Al mover una aplicación a un segundo monitor, todas las aplicaciones que forman parte de esa sesión se mueven al segundo monitor.

Cambio de aplicaciones

Muestra las aplicaciones que están abiertas dentro de una sesión.

> **Nota:**
>
> Esta opción es solo para el modo quiosco.

El selector de aplicaciones permite a los usuarios cambiar de una aplicación a otra si estas están activas en la misma sesión. Se resalta la aplicación que tiene el foco.

Modo de configuración

Para configurar, use la directiva administrativa de Google para incluir esto:

```
1 {
2
```



```
    "settings": {

        "Value": {

            "settings_version": "1.0",
                "engine_settings": {

                    "ui": {

                        "appSwitcher": {

                            "showTaskbar": true,
                            "showIconsOnly": false,
                            "autoHide": false
                                        }

                           }

                    }

         }

     }

 }


<!--NeedCopy-->
```

Lista de opciones del selector de aplicaciones, junto con sus descripciones:

- **showTaskbar**: Si se establece en true, la barra de tareas se muestra en la parte inferior de la sesión. Para ocultar la barra de tareas, establezca esta opción en false.
- **showIconsOnly**: Si se establece en true, se muestran los iconos de la barra de tareas. De forma predeterminada, la opción está establecida en false.
- **autoHide**: Si se establece en true, la barra de tareas se oculta automáticamente. De forma predeterminada, la opción está establecida en false.

Iconos de la barra de tareas

Las aplicaciones y los escritorios que se hayan configurado mediante Citrix Virtual Apps and Desktops y Citrix DaaS en una sesión activa se muestran como aplicaciones independientes. Puede ver estas aplicaciones en la barra de tareas (estantería) del dispositivo ChromeOS. Esta función se aplica a aplicaciones y escritorios publicados. El funcionamiento y el comportamiento de esta función es similar a la experiencia de barra de tareas que ofrece el sistema operativo Windows.

De manera predeterminada, esta función está habilitada.

Modo de configuración

Configuración de iconos de barra de tareas mediante la directiva administrativa de Google

> **Nota:**
>
> Citrix recomienda usar este método solo cuando se reempaquete la aplicación Citrix Workspace para ChromeOS para los usuarios.

1. Inicie una sesión en la Consola de administración de Google.
2. Vaya a **Administración de dispositivos > Administración de Chrome > Configuración de usuario**.
3. Agregue estas cadenas al archivo `policy.txt`.

```
//Preferences for chrome app
'appPrefs':{
    'chromeApp':{
        'seamless' : {
            'showInShelf' : false
        },
```

4. **Guarde** y cierre el archivo.

Configuración de iconos de barra de tareas mediante `web.config` en StoreFront

> **Nota:**
>
> Citrix recomienda usar el método del archivo `web.config` únicamente para configuraciones. Puede usar este método cuando se utilice la versión de la tienda de aplicaciones de la aplicación Citrix Workspace para ChromeOS.

1. Abra el archivo `web.config` del sitio de Citrix Receiver para Web. Este archivo está en `C:\inetpub\wwwroot\Citrix\\\\<Storename>Web`, donde `Storename` es el nombre especificado para el almacén cuando se creó.
2. Busque el campo **chromeAppPreferences** y defina su valor con la configuración como cadena JSON.

Por ejemplo:

```
chromeAppPreferences='{

    "seamless":{

        "showInShelf":false
         }

         }

<!--NeedCopy-->
```


Configuración de iconos de barra de tareas mediante el archivo configuration.js El archivo **configuration.js** se encuentra en la **carpeta raíz de ChromeApp**. Acceda a este archivo directamente para modificar la aplicación Citrix Workspace.

> **Nota:**
>
> Se necesitan credenciales de nivel de administrador para modificar el archivo configuration.js. Después de modificarlo, vuelva a empaquetar la aplicación para que las modificaciones surtan efecto.

Para cambiar la barra de tareas de ChromeOS mediante el archivo configuration.js:

1. Abra el archivo configuration.js y defina el atributo **showInShelf** como "true".

Por ejemplo:

```
//Preferences for chrome app
'appPrefs':{
    'chromeApp':{
        'seamless' : {
            'showInShelf' : false
        },
```

Limitaciones de la función:

1. Cuando se inicia más de una instancia de la misma aplicación, el icono de la aplicación no se superpone y aparece como dos iconos independientes. Por ejemplo, dos instancias del Bloc de notas muestran dos iconos del Bloc de notas en la barra de tareas.
2. No se admite la fijación de aplicaciones.

Experiencia en las sesiones

June 18, 2024

Modo de pantalla completa

Modo de configuración

Para configurar la sesión de escritorio de forma que siempre se abra en el modo de pantalla completa, modifique la directiva administrativa de Google para incluir lo siguiente:

> **Nota:**
>
> - De forma predeterminada, las sesiones de escritorio se abren en ventanas maximizadas, donde el valor "window state"está establecido en "maximized".

```
{


      "settings": {


                      "Value": {

                      "settings_version": "1.0",
                      "engine_settings": {

                      "ui": {

                      "sessionsize": {

                      "windowstate": "fullscreen"
                                }

                                        }

                                                }

                              }

                  }

 }

<!--NeedCopy-->
```

Tamaño de la sesión

Modo de configuración

Configurar el tamaño de la sesión permite personalizar las resoluciones de una sesión. Modifique la directiva administrativa de Google para incluir lo siguiente:

```
{

    "settings": {

      "Value": {

            "settings_version": "1.0",
```



```
8               "engine_settings": {
9
10              "ui": {
11
12                  "sessionsize" : {
13
14                      "minwidth" : 240,
15                      "minheigh" : 120,
16                      "available" : {
17
18                              "default" : "Fit_To_Window",
19                              "values" : [
20                                          "Fit_To_Window",
21                                          "Use_Device_Pixel_Ratio",
22                                          "1280x800",
23                                          "1440x900",
24                                          "1600x1200"
25                                      ]
26                          }
27
28                      }
29
30                  }
31
32              }
33
34          }
35
36      }
37
38  }
39
40
41  <!--NeedCopy-->
```

Lista de las diferentes opciones de resolución, junto con sus descripciones:

- **minwidth**: 240, el ancho mínimo de las sesiones.
- **minheight**: 120, la altura mínima de las sesiones.
- **available**: opciones para establecer preferencias de resoluciones para las sesiones.
  - **default**: el valor que se establezca se aplica a la resolución predeterminada. De forma predeterminada, el valor está establecido en "Fit_To_Window". Puede cambiar el valor predeterminado de la siguiente manera:
    - **values**: otros valores de resolución son:
      - **Fit_To_Window**: el valor de resolución predeterminado disponible. Coincide con el tamaño de la ventana para emular varias resoluciones de pantalla.
      - **Use_Device_Pixel_Ratio**: escala las sesiones para que coincidan con los PPP del dispositivo.
      - **1280x800**: establece el tamaño de la sesión en 1280 x 800 píxeles.

- **1440x900**: establece el tamaño de la sesión en 1440 x 900 píxeles.
- **1600x1200**: establece el tamaño de la sesión en 1600 x 1200 píxeles.

Net Promoter Score

La aplicación Citrix Workspace para ChromeOS solicita periódicamente una calificación de Net Promoter Score (NPS). En el mensaje se le pide que califique su experiencia con la aplicación Citrix Workspace para ChromeOS. Usamos los comentarios de NPS como herramienta para medir la satisfacción de los clientes y mejorar aún más la aplicación.

Puede puntuar su experiencia en una escala del 1 al 5, donde el 5 indica la mayor satisfacción.

Modo de configuración

Para configurar NPS, utilice la directiva administrativa de Google para incluir lo siguiente. Si la opción está establecida en true, el usuario puede proporcionar la calificación.

```
{

    "settings": {

        "Value": {

            "settings_version": "1.0",
                "engine_settings": {

                    "ui": {

                        "netPromoters": true
                           }

                 }

          }

     }

 }


<!--NeedCopy-->
```

Inicio automático de sesiones ICA

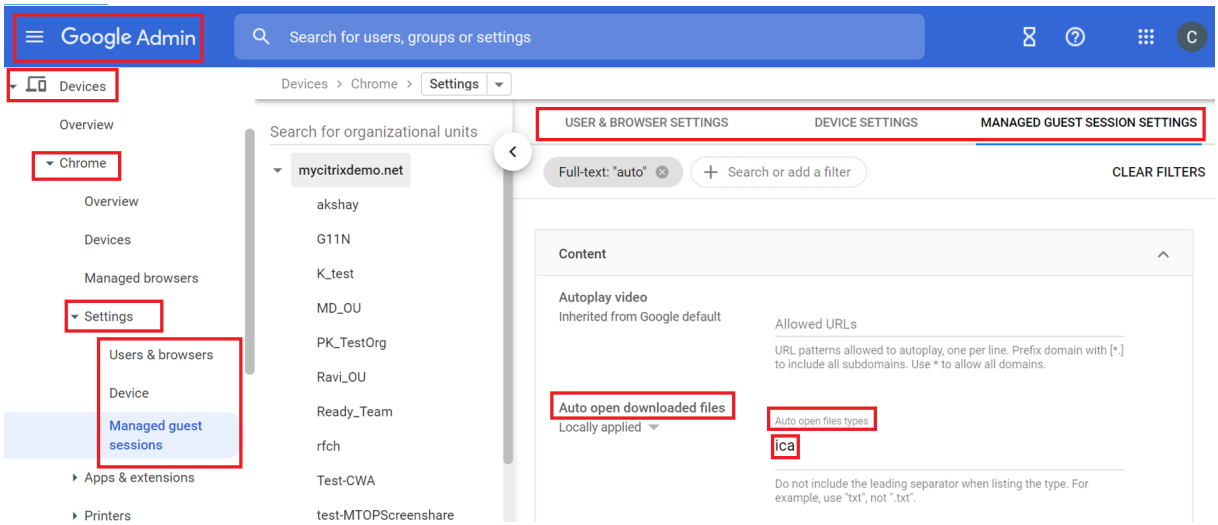
La aplicación Citrix Workspace para ChromeOS permite el inicio automático de sesiones ICA (Independent Computing Architecture) en usuarios o dispositivos administrados por Google.

Con esta función, puede acceder a recursos de forma remota desde Citrix Workspace para la web. El archivo ICA descargado se inicia automáticamente con la aplicación Citrix Workspace para ChromeOS si se instaló en el dispositivo. Antes, solo se podían descargar archivos ICA y abrirlos manualmente para iniciar los recursos. Además, los archivos ICA no se eliminaban al abrirlos y permanecían en el dispositivo. Ahora, el archivo ICA se elimina automáticamente del dispositivo una vez que se haya usado para iniciar automáticamente la sesión.

Modo de configuración

Para configurar el inicio automático de sesiones ICA, inicie sesión como administrador y siga estos pasos:

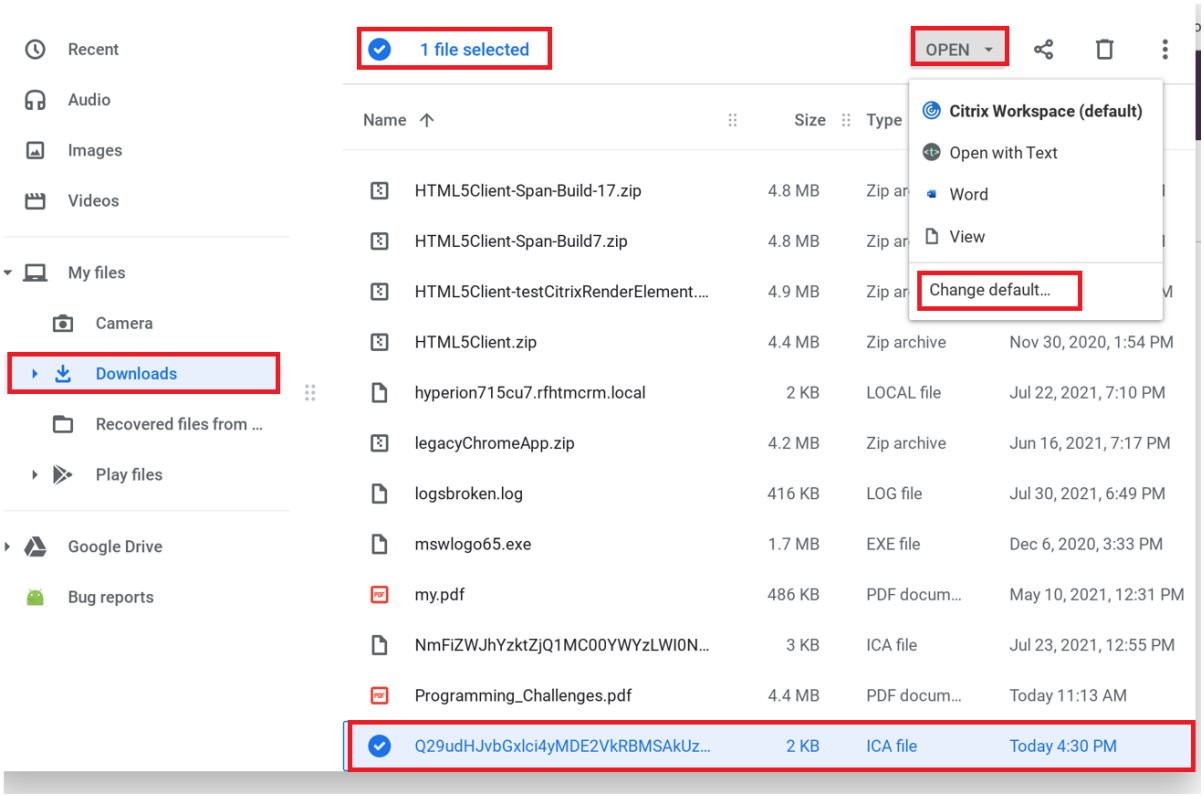
1. Inicie una sesión en la **Consola de administración de Google**.
2. En la **consola de administración de Google**, seleccione **Devices > Chrome > Settings**.
3. A continuación, en **Settings**, seleccione **Users & Browsers**, **Device** y **Managed Guest Session Settings** (como corresponda), configure **Auto-open downloaded files** y agregue **ica** en **Auto-open file types** para **User & Browser Settings**, **Device Settings**, y **Managed Guest Session Settings** como corresponda (para usuarios y dispositivos administrados).



A continuación, pida a los usuarios que asocien el archivo ICA a la aplicación Citrix Workspace para ChromeOS en sus dispositivos ChromeOS de la siguiente manera:

1. Abra **File Manager** y vaya al archivo ICA previamente descargado.
2. Haga clic en el archivo ICA.
3. En el lado derecho de la barra de navegación, haga clic en **Open** y seleccione la flecha que hay al lado.
4. A continuación, seleccione **Change default**.
5. Aparecerá una lista de las aplicaciones disponibles.

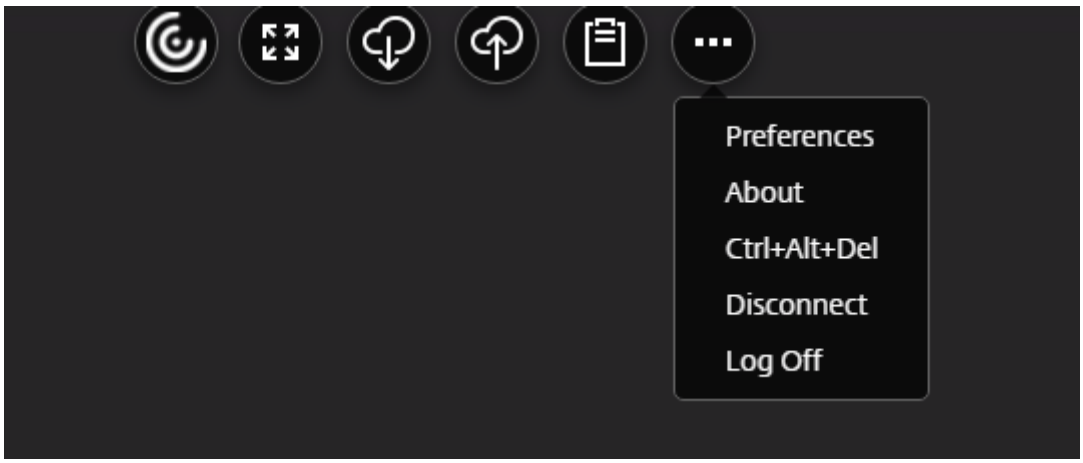
6. Seleccione **Citrix Workspace**.



Barra de herramientas y cuadros de diálogo en la sesión

La barra de herramientas de la sesión es una barra de herramientas flotante que se puede mover a cualquier parte de la pantalla. La barra de herramientas contiene el icono de la aplicación Citrix Workspace. Una barra de herramientas personalizada mejora la experiencia del usuario. Esta mejora ofrece nuevas opciones accesibles desde la barra de herramientas para facilitar tareas comunes como:

- Cambiar al modo de pantalla completa
- Cargar y descargar archivos
- Copiar contenido desde una sesión activa al portapapeles para poder compartirlo entre sesiones
- Acceder a más opciones



> **Nota:**
>
> En los dispositivos táctiles, el icono de la aplicación Citrix Workspace aparece en la parte central superior para mostrar la barra de herramientas flotante durante las sesiones de escritorio. Un botón de menú que muestra la barra de herramientas flotante se transforma en el icono de Citrix Workspace al pasar el mouse sobre él.

Modo de configuración

La barra de herramientas está habilitada de forma predeterminada.

Para ocultar o personalizar elementos individuales de la barra de herramientas, modifique la directiva administrativa de Google para incluir lo siguiente:

```
{

    "settings": {

        "Value": {

            "settings_version": "1.0",
                "engine_settings": {

                "ui" : {

                    "toolbar" : {

                            "menubar" :true,
                            "usb": true,
                            "fileTransfer":true,
                            "about":true,
                            "lock":true,
                            "disconnect":true,
                            "logoff":true,
                            "fullscreen":true,
                            "multitouch":true,
```



```
                                "preferences":true,
                                "gestureGuide":true
                                      }

                           }

                     }

            }

      }

 }


<!--NeedCopy-->
```

Lista de opciones de barra de herramientas en la sesión, junto con sus descripciones:

- **menubar**: la barra de herramientas se muestra cuando se establece en **true** y se oculta cuando se establece en **false**.
- **usb**: abre el cuadro de diálogo de dispositivos USB. Contiene la lista de dispositivos que se pueden redirigir a la sesión. Para redirigir un dispositivo USB, seleccione un dispositivo apropiado y haga clic en **Connect**.
- **fileTransfer**: función de transferencia segura de archivos entre un dispositivo de usuario y una sesión de Citrix Virtual Apps and Desktops y Citrix DaaS. Puede cargar y descargar archivos desde y hacia una sesión y acceder a los datos.
- **about**: muestra la página de licencias de terceros y proporciona el número de versión.
- **lock**: envía "Ctrl+Alt+Supr"a la sesión.
- **disconnect**: desconecta la sesión.
- **logoff**: cierra la sesión.
- **fullscreen**: ajusta la sesión al modo de pantalla completa. Si la sesión está conectada y hay varios monitores, el icono de varios monitores aparece en la barra de menús, en lugar de un icono de pantalla completa. Aparece un icono **Restore** en la barra de menús durante el modo de pantalla completa. Para volver al modo maximizado, haga clic en **Restore** en la interfaz de usuario de la barra de herramientas.
- **multitouch**: envía remotamente todos los gestos a la sesión virtual y la aplicación reacciona en función de los gestos que admite.
- **preferences**: ofrece opciones para personalizar el programa CEIP y los parámetros de resolución de las pantalla.
- **gestureGuide**: ofrece una guía de los gestos disponibles en el modo táctil.

Para ocultar la configuración de la barra de herramientas mediante el archivo configuration.js:

El archivo `configuration.js` está en la carpeta **raíz de ChromeApp**. Modifique este archivo di-

rectamente para hacer cambios en la aplicación Citrix Workspace para ChromeOS.

1. Abra el archivo configuration.js y defina el atributo "menubar"como "false".

También puede ocultar un icono individual e impedir así que se muestre en la barra de herramientas. Por ejemplo, para ocultar el botón Ctrl+Alt+Supr en la barra de herramientas:

1. Abra el archivo configuration.js y defina el atributo "lock"como "false".

> **Notas:**
>
> - Citrix recomienda hacer una copia de seguridad del archivo **configuration.js** antes de hacer cambios.
> - Citrix recomienda modificar el archivo **configuration.js** solo si la aplicación Citrix Workspace para ChromeOS se reempaqueta para los usuarios.
> - Se requieren credenciales de nivel de administrador para modificar el archivo **configuration.js**.

Sesiones compartidas

Para poder compartir sesiones, las aplicaciones deben residir en la misma máquina, deben estar configuradas en el modo de ventana integrada con los mismos parámetros (como el tamaño de la ventana, la profundidad de color y el cifrado). El uso compartido de sesiones está habilitado de manera predeterminada cuando una aplicación alojada pasa a estar disponible.

Indicador de estado de la batería

El estado de la batería del dispositivo aparece en el área de notificaciones dentro de la sesión del escritorio virtual. Antes, el indicador de estado de la batería no estaba visible en la sesión, lo que a veces afectaba a la productividad cuando el portátil se apagaba tras agotarse la batería.

Esta función solo está disponible en VDA 7.18 y versiones posteriores.

> **Nota:**
>
> - En VDA con Microsoft Windows 10, es posible que el indicador de estado de la batería tarde 1 o 2 minutos en aparecer.

Continuidad del servicio

La continuidad del servicio elimina o reduce la dependencia de la disponibilidad de los componentes involucrados en el proceso de conexión. Puede iniciar Citrix Virtual Apps and Desktops y Citrix DaaS independientemente del estado de los servicios de la nube. En otras palabras, la continuidad del

servicio le permite conectarse a las aplicaciones y escritorios de DaaS durante las interrupciones del servicio. Como requisito previo, el dispositivo debe mantener una conexión de red a una ubicación de recursos.

Para obtener más información, consulte la sección Continuidad del servicio de la documentación de Citrix Workspace.

> **Notas:**
>
> - La función de continuidad del servicio está inhabilitada.
> - Si anteriormente habilitó la función de continuidad del servicio y está usando una versión anterior de la aplicación Citrix Workspace para ChromeOS, es posible que no pueda usar la continuidad del servicio. Para habilitar esta función, se recomienda actualizar la aplicación Citrix Workspace a la versión más reciente (2402.1 o posterior) y seguir las instrucciones del artículo CTX632723de Knowledge Center.

Configuración

Puede habilitar la función de continuidad del servicio de esta manera:

- Directiva administrativa de Google

Directiva administrativa de Google Para los usuarios y dispositivos administrados, los administradores pueden habilitar la función de continuidad del servicio mediante la directiva administrativa de Google de esta manera:

1. Inicie sesión en la directiva administrativa de Google.
2. Puede aplicar esta configuración a lo siguiente:
   - **Dispositivo** > **Chrome** > **Aplicaciones y extensiones** > **Usuarios y exploradores** > busque la extensión > Política de extensiones.
   - **Dispositivo** > **Chrome** > **Aplicaciones y extensiones** > **Quioscos** > Buscar la extensión > Política de extensiones.
   - **Dispositivo** > **Chrome** > **Aplicaciones y extensiones** > **Sesiones de invitados gestionadas** > Buscar la extensión > Política de extensiones.

   A continuación se muestra un ejemplo de datos JSON:

```
{

"settings": {

    "Value": {

```



```
        "settings_version": "1.0",
        "engine_settings": {

            "features": {

                "serviceContinuity":{

                    "enable": true
                     }

                 }

              }

          }

      }

 }


<!--NeedCopy-->
```

Redirección de contenido del explorador web

La redirección de contenido del explorador web (BCR) redirige el contenido del explorador web remoto al dispositivo del cliente. BCR es un explorador web sin bordes ni marcos que se ejecuta dentro de la ventana del escritorio remoto y cubre (se superpone) el área de contenido del explorador web remoto (VDA).

BCR redirige el contenido de un explorador web a un dispositivo cliente y crea un explorador web correspondiente incrustado en la aplicación Citrix Workspace. Esta funcionalidad reduce el uso de red, el procesamiento de páginas y la generación de gráficos para el dispositivo de punto final. Por tanto, mejora la experiencia del usuario cuando este visita páginas web con contenido sofisticado, especialmente aquellas páginas web que contienen HTML5 o WebRTC. Solo la ventanilla (la parte visible para el usuario en la página web) se redirige al dispositivo de punto final. La redirección de contenido de explorador no redirige la interfaz de usuario (la barra de direcciones, la barra de herramientas, etc.) del explorador en el VDA.

En otras palabras, BCR ofrece la posibilidad de generar páginas web incluidas en la lista de permitidos en el lado del cliente. Esta función utiliza la aplicación Citrix Workspace para crear una instancia de motor de generación correspondiente en el lado del cliente, que obtiene el contenido HTTP y HTTPS a partir de la URL.

Para obtener más información sobre cómo configurar la lista de permitidos, consulte:

- Extensión de Chrome de redirección de contenido de explorador web

- Configuración de directiva Redirección de contenido de explorador web

Problemas conocidos de la función

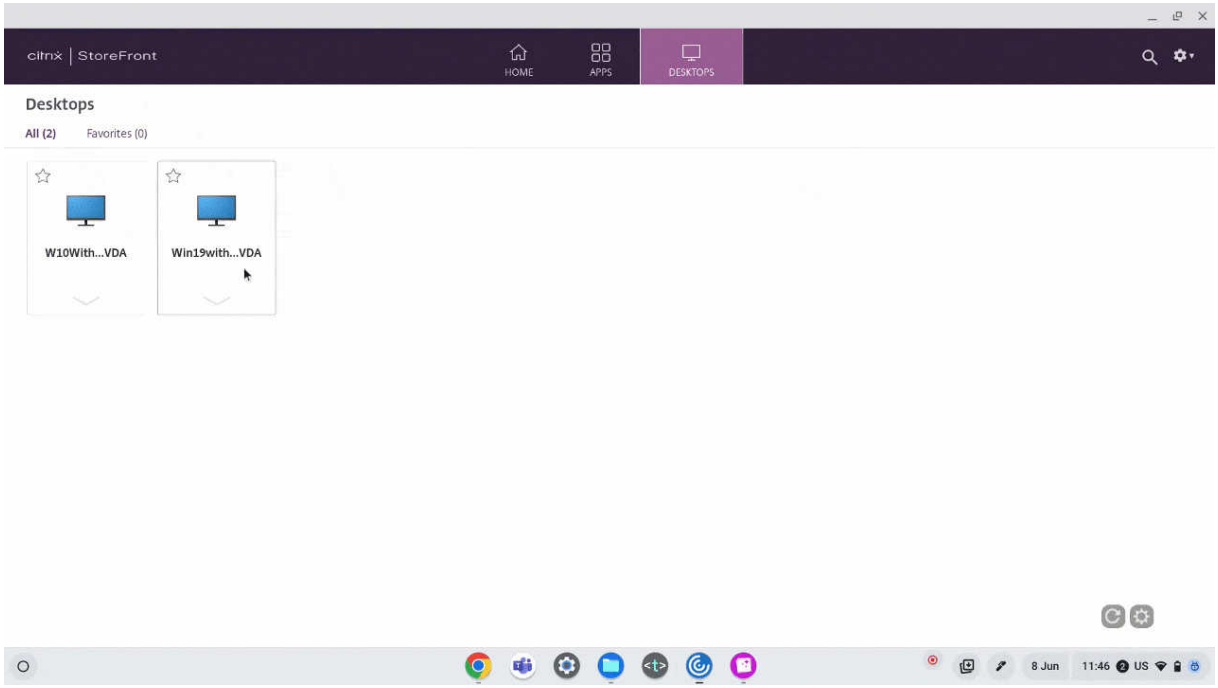
- En la superposición de la redirección BCR, al abrir un enlace a un sitio web en una ficha nueva, este se abre en el explorador web del cliente en lugar de abrirse en el explorador web de la sesión. [HDX-43206]

Limitaciones conocidas de la función

- Esta función no admite:
  - Casos de obtención en el servidor y generación en el cliente.
  - Servidores web de autenticación integrada de Windows (IWA).
  - Función de varios monitores.
- Al cargar o descargar archivos en algunos de los sitios web redirigidos por BCR, aparece el selector de archivos de ChromeOS en lugar del selector de archivos de la sesión de VDA. [HDX-43207]
- No se admite la impresión desde páginas redirigidas por BCR.

Experiencia mejorada al iniciar aplicaciones y escritorios virtuales

A partir de la versión 2306, la experiencia mejorada en el inicio de aplicaciones y escritorios proporciona información oportuna y relevante sobre el estado del inicio.



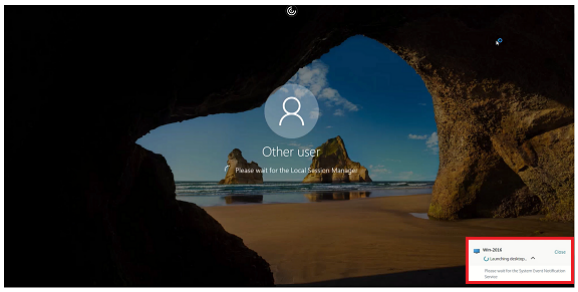
Configurar la pantalla de notificaciones de inicios de sesión

A partir de 2307, los administradores pueden habilitar o inhabilitar la visualización de las notificaciones de progreso de inicio mediante la siguiente configuración.

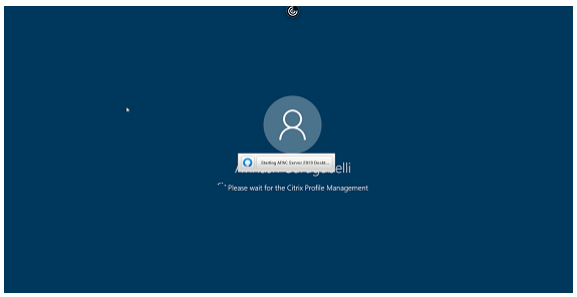
Si esta configuración está habilitada, puede ver las notificaciones de progreso del inicio de las sesiones en la parte inferior derecha de la pantalla. Si esta configuración está inhabilitada, no podrá ver las notificaciones de progreso del inicio de las sesiones.

> **Nota:**
>
> - De forma predeterminada, esta configuración está habilitada.

Cuando las notificaciones están inhabilitadas, los usuarios finales carecen de la información oportuna y relevante sobre el estado de los inicios.



Cuando las notificaciones están habilitadas, los usuarios finales ven el progreso de los inicios en la parte inferior derecha de la pantalla.



Configuraciones Puede configurar esta función de una de estas maneras:

- Configuration.js
- Directiva administrativa de Google

Configuration.js Para inhabilitar esta función mediante el archivo **configuration.js**, haga lo siguiente:

1. Busque el archivo **configuration.js** en la carpeta **raíz de ChromeApp**.

2. Modifique el archivo.

> **Notas:**
>
> - Citrix recomienda hacer una copia de seguridad del archivo **configuration.js** antes de hacer cambios.
> - Citrix recomienda modificar el archivo **configuration.js** solo si la aplicación Citrix Workspace para ChromeOS se reempaqueta para los usuarios.
> - Se requieren credenciales de nivel de administrador para modificar el archivo **configuration.js**.

3. Establezca el valor de **CTXTUI** en **false** para inhabilitar la visualización de las notificaciones de progreso de los inicios.
   A continuación se muestra un ejemplo de datos JSON:

```
{

"vc_channel":{

    "CTXTUI": false
     }

 }

<!--NeedCopy-->
```

4. Guarde los cambios.

Directiva administrativa de Google Para los usuarios y dispositivos administrados, los administradores pueden inhabilitar esta función mediante la directiva administrativa de Google de esta manera:

1. Inicie sesión en la directiva administrativa de Google.
2. Vaya a **Administración de dispositivos** > **Administración de Chrome** > **Configuración de usuario**.
3. Agregue estas cadenas al archivo **policy.txt** en la clave **engine_settings**.

   A continuación se muestra un ejemplo de datos JSON:

```
{

    "settings": {

        "Value": {

            "settings_version": "1.0",
            "engine_settings": {
```



```
 9
10                  "vc_channel":
11
12 {
13                        "CTXTUI": false                    }
14
15
16                }
17
18            }
19
20        }
21
22  }
23
24 <!--NeedCopy-->
```

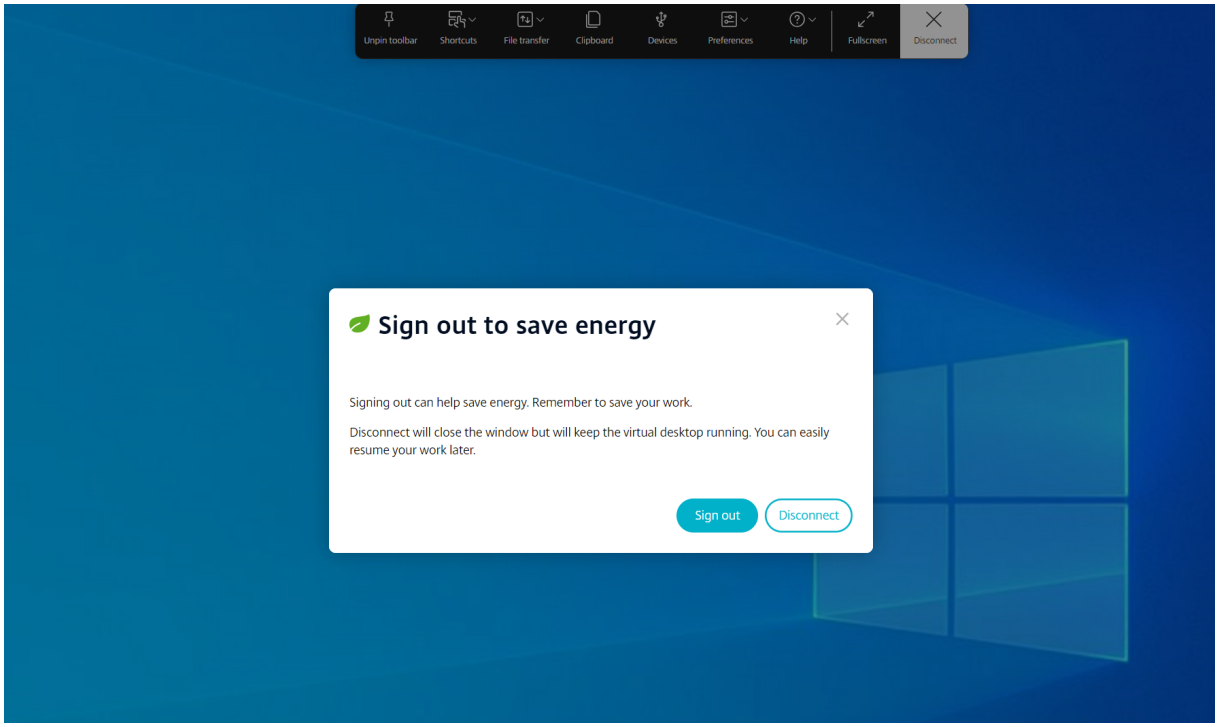
4. Guarde los cambios.

Iniciativa de sostenibilidad de la aplicación Citrix Workspace

Anteriormente, los escritorios virtuales permanecían en estado desconectado cuando los usuarios los cerraban tocando el botón "X". Eso consumía energía y recursos energéticos innecesarios.

A partir de la versión 2405, hemos introducido una iniciativa de sostenibilidad que anima a los usuarios a ahorrar la energía que se podría desperdiciar al ejecutar escritorios virtuales no utilizados.

Con esta función habilitada, cuando los usuarios tocan el icono **X** para desconectar la sesión, se muestra un mensaje para cerrar sesión en la sesión de escritorio. Esta función puede resultar útil en las empresas que usan directivas del sistema operativo Windows para apagar las máquinas virtuales cuando no hay usuarios con sesiones iniciadas.



Los usuarios finales pueden salir de la sesión de dos maneras:

Cerrar sesión para ahorrar energía: Esta acción de sostenibilidad apaga la máquina virtual y ahorra energía. Los usuarios finales deben asegurarse de guardar su trabajo antes de cerrar sesión.

Desconectar para cerrar la ventana de sesión del escritorio virtual. No obstante, la sesión virtual permanece activa hasta el siguiente inicio de sesión. Los usuarios finales pueden reanudar su trabajo fácilmente.

Experiencia en los almacenes

May 16, 2024

Parámetros del almacén

Modo de configuración

Para crear un almacén, identifique y configure las comunicaciones con los servidores. Puede proporcionar los recursos que deberán estar disponibles en el almacén. A continuación, opcionalmente, configure el acceso remoto al almacén a través de Citrix Gateway. Para configurar el almacén, utilice la directiva administrativa de Google para incluir lo siguiente:


```
{

    "settings": {

        "Value": {

            "settings_version": "1.0",
            "store_settings": {

                "name": "SampleStore",
                "gateways": [{

                    "url": "https: //yourcompany.gateway.com",
                    "is_default": true
                 }
 ],
                "beacons": {

                    "internal": [{

                        "url": "http: //yourcompany.internalwebsite.net
                            "
                     }
 ],
                    "external": [{

                        "url": "http: //www.yourcompany.externalwebsite
                            .com"
                     }
 ]
                 }
 ,
                "rf_web": {

                    "url": "http: //yourcompany.storefrontstoreweb.net"
                 }

             }

          }

      }

 }


<!--NeedCopy-->
```

Lista de opciones de configuración del almacén, junto con sus descripciones:

- “name”: Introduzca el nombre del almacén.
- “gateways”: Direcciones URL de la puerta de enlace.

Agregue direcciones URL de la puerta de enlace en el formato `https://gateway.domain.com` o `https://yourcompany.gateway.com` y haga clic en **Agregar** en la página de la utilidad.

Puede establecer una puerta de enlace predeterminada si se agregan dos o más direcciones URL de puerta de enlace.

Para que una puerta de enlace sea la predeterminada, establezca el indicador "is_default"en true. De lo contrario, establezca el indicador en false.

Por ejemplo:

```
    {

        "settings": {

            "Value": {

            "settings_version": "1.0",
            "store_settings": {

                "name": "RTST",
                    "gateways": [{

                        "url": "https: //yourcompany.gateway.com"
                            ,
                        "is_default": true
                    }
,
                    {

                        "url": "https://gateway2.domain.com",
                        "is_default": false
                    }
]
                }

        }

    }

 }


<!--NeedCopy-->
```

- "internal": Determina si la aplicación Citrix Workspace se conecta a StoreFront directamente o a través de una puerta de enlace. Por ejemplo, `https://storefront.domain.com`.
- "external": Determina si la interfaz de red especificada está disponible y permite el tráfico. Por ejemplo, `https://citrix.com`.

- “rf_web”: Dirección URL del almacén.

Compatibilidad con varios almacenes

A partir de la versión 2305, los administradores de TI pueden asignar varios almacenes a los usuarios finales. Ahora, es fácil para los usuarios finales cambiar entre almacenes sin necesidad de recordar su URL exacta. Esta función mejora la experiencia del usuario al acceder a varios almacenes.

Modo de configuración

Para configurar varios almacenes, los administradores de TI pueden modificar la directiva administrativa de Google. A continuación se muestra un ejemplo de datos JSON:

```
{

      "settings_version": "1.0",
      "store_settings": {

            "name": "SampleStore",
            "gateways": [{

                  "url": " https: //yourcompany.gateway.com",
                  "is_default": true
             }
 ],
            "beacons": {

                  "internal": [{

                        "url": " http: //yourcompany.internalwebsite.
   net"
                   }
 ],
                  "external": [{

                  "url": " http: //www.yourcompany.externalwebsite.com"
                   }
 ]
             }
 ,
            "rf_web": {

                  "url": " http: //yourcompany.storefrontstoreweb.net"
             }
 ,
            "secondary_stores": [{

                  "name": " SampleStore",
                  "gateways": [{
```



```
36
37                          "url": " https: //yourcompany.gateway.com ",
38                          "is_default": true
39                      }
40  ],
41                     "beacons": {
42
43                          "internal": [{
44
45                          "url": " http: //yourcompany.internalwebsite.
      net "
46                           }
47  ],
48                          "external": [{
49
50                       "url": " http: //www.yourcompany.externalwebsite.
      com "
51                           }
52  ]
53                      }
54  ,
55                     "rf_web": {
56
57                     "url": " http: //yourcompany.storefrontstoreweb.net "
58                      }
59
60                 }
61  , {
62
63                     "rf_web": {
64
65                     "url": " http: //yourcompany.storefrontstoreweb.net "
66                      }
67
68                 }
69  ]
70         }
71
72  }
73
74  <!--NeedCopy-->
```

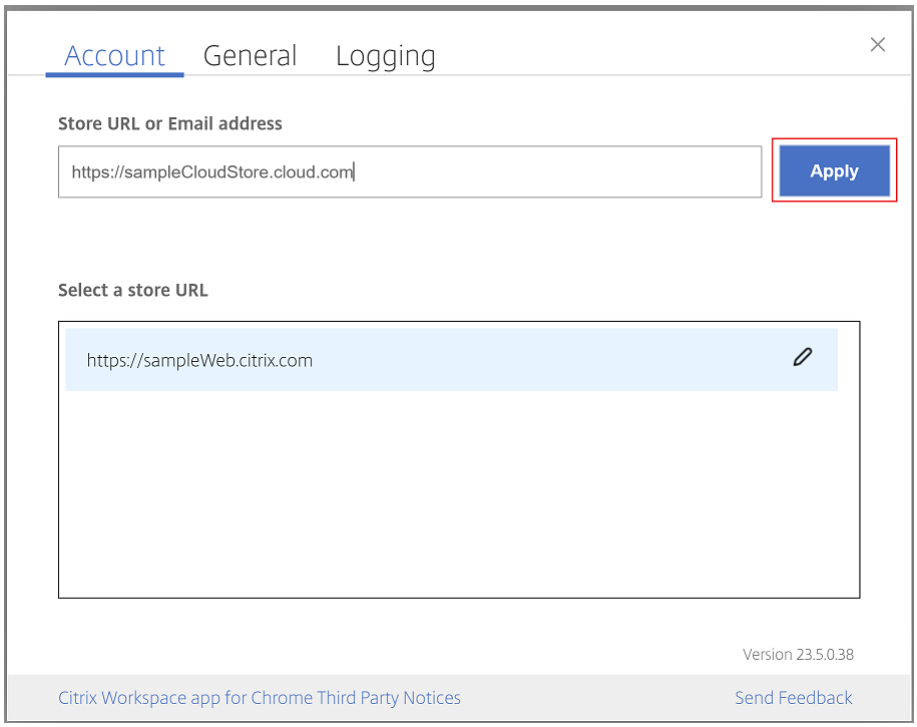
El atributo **secondary_stores** permite configurar varios almacenes. Un administrador puede usar la estructura JSON varias veces. Para obtener más información sobre cómo personalizar la aplicación Citrix Workspace para ChromeOS, consulte la herramienta de utilidad de configuración.

Varios almacenes de StoreFront

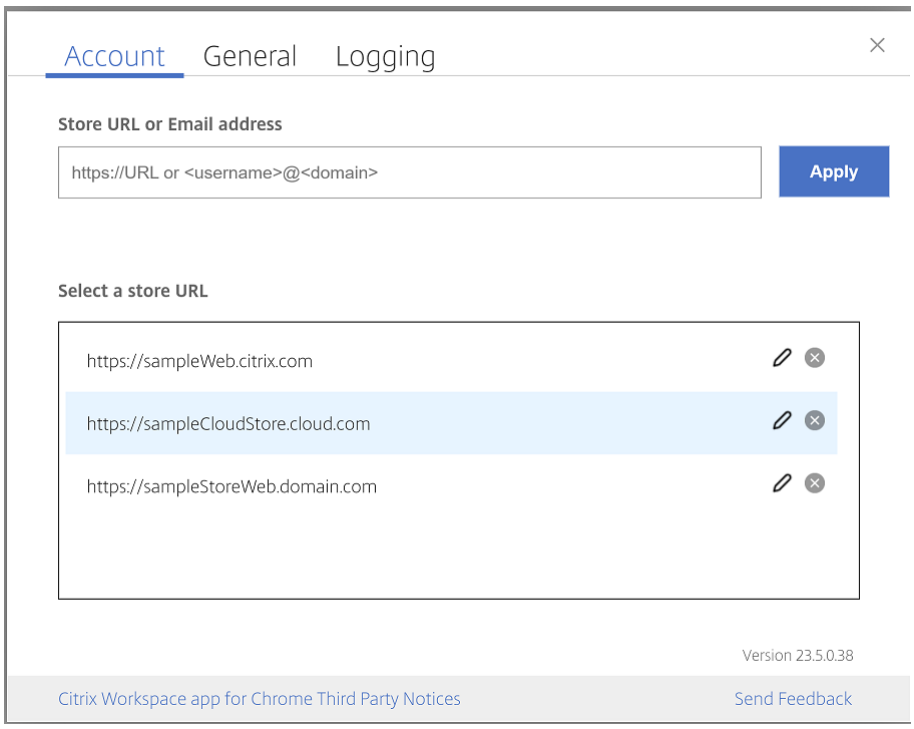
Puede cambiar la dirección del almacén sin tener que reiniciar Citrix Workspace. Las sesiones existentes de Citrix Workspace, si las hubiera, siguen ejecutándose sin interrupciones.

Para agregar almacenes:

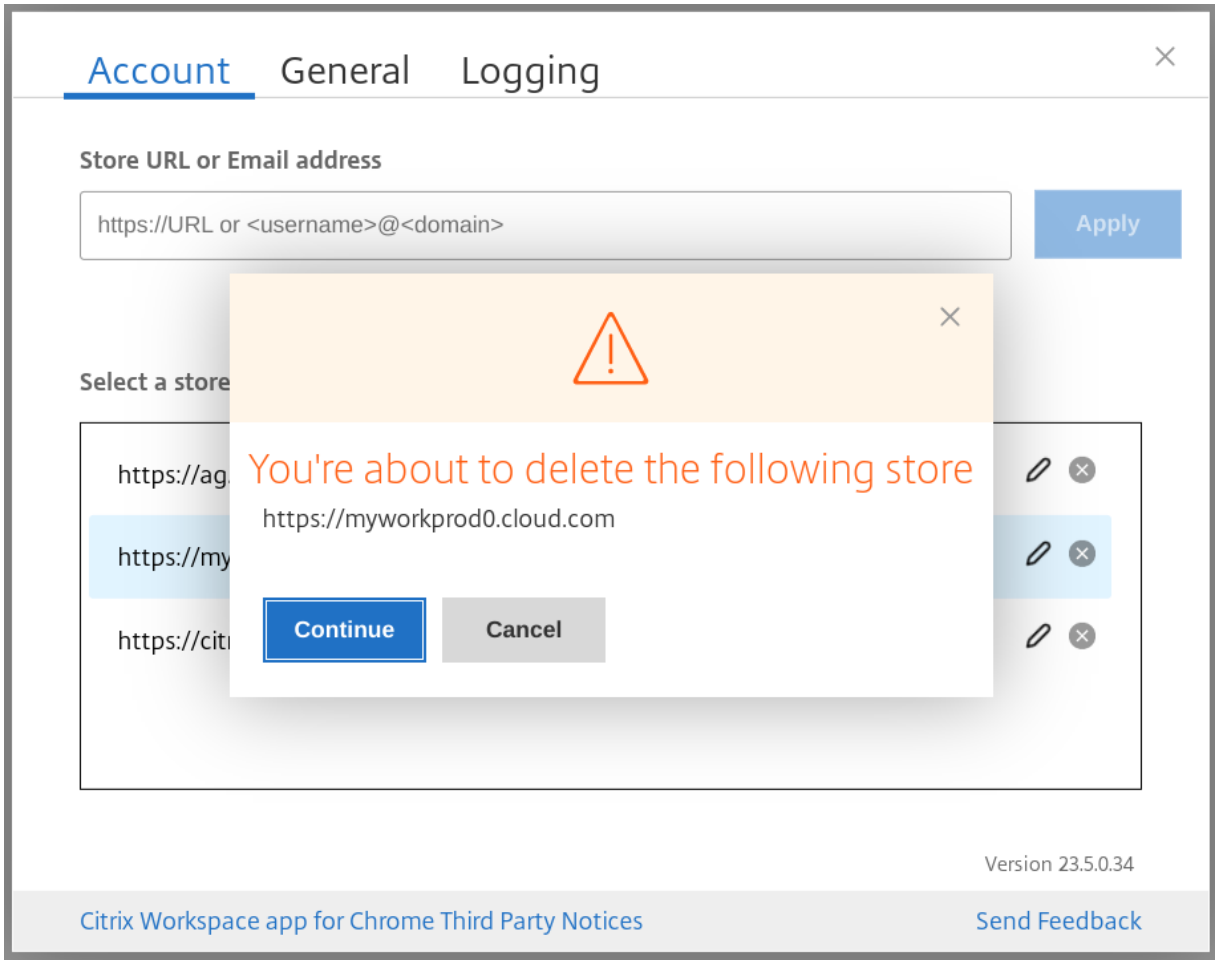
1. Haga clic en **Parámetros** en la aplicación Citrix Workspace para ChromeOS y seleccione la ficha **Cuenta**.
2. Introduzca la dirección de correo electrónico o la URL de StoreFront en el campo **URL de almacén o dirección de correo electrónico**.
3. Haga clic en **Aplicar** para guardar el nuevo almacén.



Para cambiar de almacén, seleccione uno en la lista **Seleccione una URL de almacén**.



Para quitar un almacén de la lista, haga clic en el icono **Eliminar** junto a la dirección del almacén que quiere eliminar y confirme la operación.



Volver a cargar el almacén

En la ventana de la aplicación Citrix Workspace para ChromeOS se agregó un botón para la operación de recarga. Al hacer clic en el botón, las cookies del almacén se borran y la página del almacén vuelve a cargarse.

Actualizar almacén

A partir de la versión 2307, puede aplicar estas configuraciones para evitar la duplicación de instancias de las aplicaciones publicadas.

> **Nota:**
>
> - De forma predeterminada, la configuración está inhabilitada. Al habilitar esta configuración, no verá las instancias duplicadas de la aplicación publicada. Haga clic en el icono para actualizar el almacén.

Puede configurar esta función de una de estas maneras:

• Configuration.js
• Directiva administrativa de Google

Configuration.js

Para habilitar esta función mediante el archivo **configuration.js**, haga lo siguiente:

1. Busque el archivo **configuration.js** en la carpeta **raíz de ChromeApp**.

   > **Notas:**
   >
   > - Citrix recomienda hacer una copia de seguridad del archivo **configuration.js** antes de hacer cambios.
   > - Citrix recomienda modificar el archivo **configuration.js** solo si la aplicación Citrix Workspace para ChromeOS se reempaqueta para los usuarios.
   > - Se requieren credenciales de nivel de administrador para modificar el archivo **configuration.js**.

2. Modifique el archivo y establezca **refreshStore** en **true**.

   A continuación se muestra un ejemplo de datos JSON:

   ```
   'ui' :{

     'refreshStore': true
    }

   <!--NeedCopy-->
   ```

3. Guarde los cambios.

Directiva administrativa de Google

Para los usuarios y dispositivos administrados, los administradores pueden habilitar esta función mediante la directiva administrativa de Google de esta manera:

1. Inicie sesión en la directiva administrativa de Google.
2. Vaya a **Administración de dispositivos** > **Administración de Chrome** > **Configuración de usuario**.
3. Agregue estas cadenas al archivo **policy.txt**, en **engine_settings**.

> **Nota:**
>
> También puede aplicar esta configuración en lo siguiente:
>
> - **Dispositivo** > **Chrome** > **Aplicaciones y extensiones** > **Quioscos** > Buscar la extensión > Política de extensiones.
> - **Dispositivo** > **Chrome** > **Aplicaciones y extensiones** > **Sesiones de invitados gestionadas** > Buscar la extensión > Política de extensiones.

A continuación se muestra un ejemplo de datos JSON:

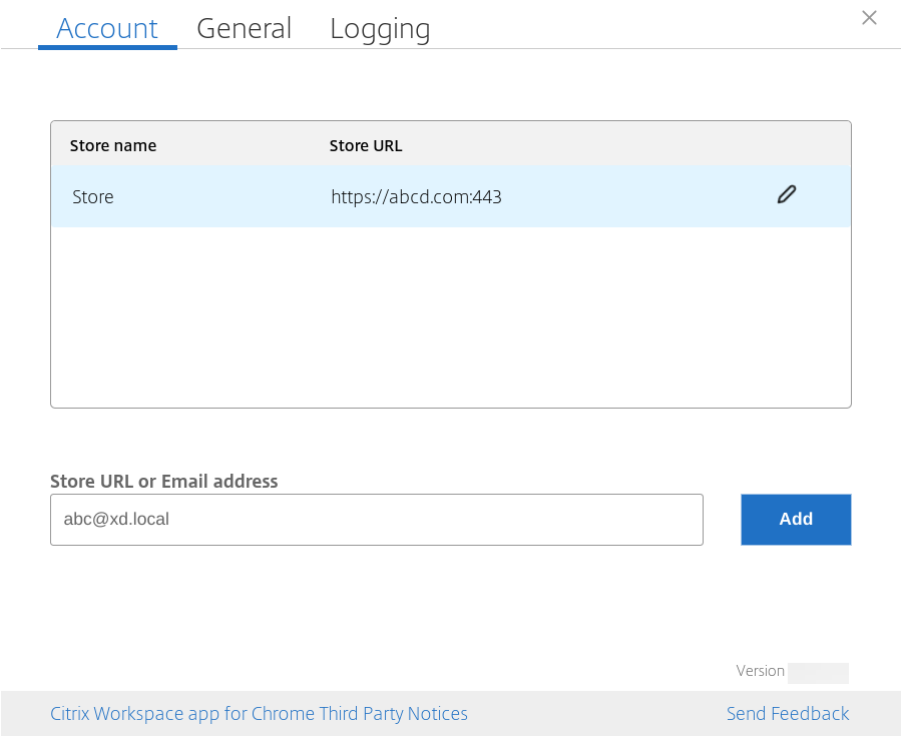
```
{

"settings": {

"Value": {

  "settings_version": "1.0",
  "engine_settings": {

    "ui": {

      "refreshStore": true
         }

       }

     }

    }

 }

<!--NeedCopy-->
```

4. Guarde los cambios.

Detección de almacenes por correo electrónico

Ahora puede usar su ID de correo electrónico para acceder a la aplicación Citrix Workspace sin necesidad de memorizar la URL del almacén. Los almacenes asignados a su cuenta se rellenan automáticamente. Vaya al menú desplegable **Cuentas** > **URL de almacén o Dirección de correo electrónico** para ver la lista de los almacenes asociados a su correo electrónico.

> **Nota:**
>
> Puede seguir usando la URL del almacén para iniciar sesión.



Como administrador, para mantener y rellenar automáticamente las cuentas de almacén, consulte Citrix Cloud API Overview como requisito previo.

Para obtener más información, consulte Global App Configuration Service.

Nombre abreviado de la URL del almacén

Anteriormente podía ver las URL de los almacenes, pero no existía la posibilidad de agregar o modificar un nombre corto para las URL de almacén. Esta disposición dificultaba que los administradores y los usuarios recordaran las URL de almacén.

A partir de la versión 2402, para los usuarios administrados, los administradores pueden insertar un nombre de almacén personalizado junto con la URL del almacén desde la consola de administración de Google. Esta función facilita a los usuarios la identificación de los diferentes almacenes. Además, el administrador puede decidir si el usuario puede modificar el nombre del almacén o no estableciendo el atributo **allowEditStoreName** en **true** o en **false**. Para obtener más información, consulte la sección de configuración.

Para los usuarios de BYOD, el nombre del almacén se genera automáticamente. Por ejemplo, Almacén, Almacén 1, Almacén 2, etc. Los almacenes se rellenan mediante la función Detección de almacenes por correo electrónico. Los usuarios pueden modificar el nombre del almacén según sea necesario.

Configuración

De forma predeterminada, los usuarios de BYOD pueden modificar el nombre del almacén.

En el caso de los dispositivos y usuarios administrados, los administradores pueden establecer el atributo **allowEditStoreName** en **true** para habilitar la función mediante la consola de administración de Google de la siguiente manera.

> **Nota:**
>
> - De forma predeterminada, el atributo **allowEditStoreName** se establece en **false**.

Directiva administrativa de Google Para habilitar esta directiva, haga lo siguiente:

1. Inicie sesión en la Consola de administración de Google.
2. También puede aplicar esta configuración en lo siguiente:
   - **Dispositivo** > **Chrome** > **Aplicaciones y extensiones** > **Usuarios y exploradores** > busque la extensión > Política de extensiones.
   - **Dispositivo** > **Chrome** > **Aplicaciones y extensiones** > **Quioscos** > Buscar la extensión > Política de extensiones.
   - **Dispositivo** > **Chrome** > **Aplicaciones y extensiones** > **Sesiones de invitados gestionadas** > Buscar la extensión > Política de extensiones.

   A continuación se muestra un ejemplo de datos JSON:

```
{

"settings": {

    "Value": {

        "settings_version": "1.0",
        "store_settings": {

            "name": "Citrix store",
            "allowEditStoreName": true,
            "rf_web":
               {

                "url": "https://xyz.cloud.com"
                                                    }

                }
 ,
         }

     }
```



```
22
23   }
24
25 <!--NeedCopy-->
```

3. Guarde los cambios.

> **Nota**:
>
> En el fragmento de código, el atributo **name** hace referencia al nombre abreviado del almacén.

Cómo utilizar la función De forma predeterminada, los usuarios de BYOD pueden modificar el nombre del almacén. Para los usuarios administrados, si el administrador de su organización otorga permiso para modificar el nombre del almacén, puede hacer lo siguiente: Para obtener más información, consulte Nombre abreviado de la URL del almacén.

Uso táctil y móvil

May 16, 2024

Modo multitoque

La aplicación Citrix Workspace para ChromeOS le permite establecer el modo **Multitoque** como el modo predeterminado a través de la Consola de administración de Google. El modo Multitoque controla la activación de los gestos multitoque.

Puede alternar entre el modo Panorámico y el modo Multitoque. Antes, el modo Panorámico era el modo predeterminado.

Al iniciar una sesión en un dispositivo táctil, los gestos se controlan de forma predeterminada en el modo Panorámico. Puede cambiar al modo Multitoque desde la barra de herramientas. Esta función ofrece una mejor experiencia de usuario.

Modo de configuración

Para establecer la función como predeterminada, modifique la directiva de la **Consola de administración de Google** y establezca el valor de **defaultMode** en **multitouch**.

```
1 {
2
3     "settings": {
4
```



```
        "Value": {

            "settings_version": "1.0",
                        "engine_settings": {

                            "ui": {

                                "touch" : {

                                    "defaultMode" : "multitouch"
                                     }

                                }

                            }

                        }

                    }


<!--NeedCopy-->
```

Compatibilidad táctil

Ahora la aplicación Citrix Workspace para ChromeOS mejora la compatibilidad táctil al permitirle ejecutar sesiones en dispositivos Chrome táctiles en modo tableta. Esta función incluye compatibilidad con gestos, funciones multitoque y teclado en pantalla.

Ahora el icono de **apertura del teclado** aparece en la barra de herramientas de la sesión cuando un dispositivo Chrome se halla en modo tableta. Al utilizar esta función o hacer un toque con tres dedos, aparece el teclado en pantalla.

Mejoras de gestos en dispositivos táctiles

A partir de la versión 23.4.0, la aplicación Citrix Workspace mejora la experiencia del usuario final en relación con los gestos, la funcionalidad multitoque y el teclado en pantalla (modo tableta). En las sesiones de la aplicación Citrix Workspace, puede utilizar todos los gestos de multitoque habituales, como tocar, deslizar o arrastrar.

Esta es la guía de gestos:

Para hacerlo:	En la aplicación Citrix Workspace, haga lo siguiente:
Un clic	Tocar con un dedo
Clic con el botón secundario	Tocar, mantener y soltar
Abrir el teclado en pantalla	Tocar con tres dedos (o, desde la barra de herramientas, tocar el icono **Teclado**)
Arrastrar	Tocar, mantener y deslizar
Habilitar el cursor	Tocar con dos dedos

Visualización automática del teclado

Puede habilitar la visualización automática del teclado en un servidor mediante el botón flotante del teclado que aparece en los campos de entrada de texto. Para que la función de visualización automática del teclado esté disponible, compruebe que el parámetro del servidor esté habilitado.

Limitaciones de la función:

- Los toques con tres dedos para obtener el teclado en pantalla no funcionan en modo multitoque. Funciona solo en modo panorámico.
- Para que el teclado en pantalla funcione correctamente, ciérrelo siempre con el icono Abrir teclado de la barra de herramientas de la sesión, en lugar del teclado en pantalla del sistema. Si utiliza el teclado en pantalla del sistema para cerrarlo, es posible que funcione de manera imprevista.

Modo de configuración

Para habilitar este parámetro, siga estos pasos:

1. En el Delivery Controller, abra Citrix Studio.
2. Seleccione **Directivas**.
3. Haga clic en **Crear directiva**.
4. Busque **Visualización automática del teclado** y seleccione **Permitido**.

Redirección de URL

May 16, 2024

Redirección del host al cliente

La redirección de contenido permite controlar si los usuarios acceden a la información:

- Mediante aplicaciones que se publican en servidores
- O mediante aplicaciones ejecutadas localmente en los dispositivos de los usuarios

La redirección del host al cliente es un tipo de redirección de contenido. Solo está disponible en VDA de SO de servidor (no en VDA de SO de escritorio) con la versión 7.15 LTSR de Citrix XenApp y XenDesktop y posteriores.

Para obtener más información, consulte Redirección de host a cliente: XenApp y XenDesktop en la documentación de XenApp y XenDesktop.

Cuando la redirección del host al cliente está habilitada, las direcciones URL se interceptan en el servidor VDA y se envían al dispositivo de usuario. La aplicación Citrix Workspace para ChromeOS muestra un cuadro de diálogo en el que se pide al usuario que elija abrir la URL en la sesión o en el dispositivo local. El cuadro de diálogo aparece para cada URL.

Cuando la redirección del host al cliente está inhabilitada, los usuarios pueden abrir las URL con exploradores web o reproductores multimedia que residan en el VDA de servidor. Cuando la redirección de host a cliente está habilitada, los usuarios no pueden inhabilitarla.

Antes, la redirección del host al cliente se llamaba redirección del servidor al cliente.

Para obtener más información, consulte Redirección de contenido general en la documentación de Citrix Virtual Apps and Desktops.

Mejoras en la redirección de URL

Anteriormente, cuando estaba habilitada la redirección de host a cliente, las URL se interceptaban en el VDA del servidor y se enviaban al dispositivo del usuario. La aplicación Citrix Workspace para ChromeOS mostraba un cuadro de diálogo en el que se pedía al usuario que eligiera abrir la URL en la sesión o en el dispositivo local. Aparecía el cuadro de diálogo para cada URL.

A partir de la versión 2305, los administradores pueden configurar la redirección de URL para abrir los enlaces en el dispositivo local sin que aparezcan cuadros de diálogo extra. De esta forma, mejora la experiencia del usuario.

> **Nota:**
>
> - De forma predeterminada, esta función está inhabilitada.

Modo de configuración

Puede habilitar esta función de una de estas maneras:

- Configuration.js
- Directiva administrativa de Google

Configuration.js Para habilitar esta función mediante el archivo **configuration.js**, haga lo siguiente:

1. Busque el archivo **configuration.js** en la carpeta raíz de **ChromeApp**.

   > **Notas:**
   >
   > - Citrix recomienda hacer una copia de seguridad del archivo **configuration.js** antes de hacer cambios.
   > - Citrix recomienda modificar el archivo **configuration.js** solo si la aplicación Citrix Workspace para ChromeOS se reempaqueta para los usuarios.
   > - Se requieren credenciales de nivel de administrador para modificar el archivo **configuration.js**.

2. Modifique el archivo **configuration.js** y establezca el valor predeterminado de **forceOpenInClient** en **true**. A continuación se muestra un ejemplo de datos JSON:

```
{

"features": {

        "UrlRedirection": {

        "forceOpenInClient": true
             }

    }

 }

<!--NeedCopy-->
```

3. Guarde los cambios.

Directiva administrativa de Google En la implementación local, los administradores pueden habilitar esta función mediante la directiva administrativa de Google de la siguiente manera:

1. Inicie sesión en la directiva administrativa de Google.
2. Vaya a **Administración de dispositivos** > **Administración de Chrome** > **Configuración de usuario**.
3. Agregue estas cadenas al archivo **policy.txt** en la clave **engine_settings**. A continuación se muestra un ejemplo de datos JSON:


```
{

  "features": {

    "UrlRedirection": {

        "forceOpenInClient": true
                    }

          }

}

<!--NeedCopy-->
```

4. Guarde los cambios.

Canales virtuales

May 16, 2024

Acerca de los canales virtuales

Un canal virtual es un controlador virtual del lado del cliente que se comunica con una aplicación del lado del servidor. Los canales virtuales son una parte necesaria de la experiencia informática remota de los servidores de Citrix Virtual Apps and Desktops.

Los canales virtuales se utilizan en los siguientes aspectos:

- Impresión
- Asignación de puertos serie
- Portapapeles
- Audio
- Contenido multimedia
- Canal de control
- EUEM
- USB
- Transferencia de archivos
- Movilidad
- Multitoque
- Tarjeta inteligente
- Receiver para móviles

- Microsoft Teams
- Editor de métodos de entrada
- Redirección de contenido del explorador web
- Asignación de unidades del cliente
- Interfaz de usuario transparente

Modo de configuración

Todos los canales virtuales están habilitados de forma predeterminada. Para inhabilitar un canal virtual concreto, utilice la directiva administrativa de Google para incluir lo siguiente. Seleccione el nombre de la función en "vc_channel"y haga clic en **Add** en la página de la utilidad. Por ejemplo:

```
{

    "settings": {

        "Value": {

            "settings_version": "1.0",
                "engine_settings": {

                        "vc_channel": {

                            "<vc_name1>": false,
                            "<vc_name2>": false,
                            "<vc_name3>": false,
                            "<vc_namen>": false
                                        }

                                }

          }

      }

 }


<!--NeedCopy-->
```

Para habilitar un "vc_channel"concreto, seleccione la función y haga clic en **Remove** en la página de la utilidad.

> **Nota:**
>
> Los nombres pueden ser de 1 a n. El apellido "n"no puede tener una coma después de establecerlo en true o false.

```
{
```



```
2
3     "settings": {
4
5         "Value": {
6
7             "settings_version": "1.0",
8                 "engine_settings": {
9
10                    "vc_channel": {
11
12                        "CTXCPM ": false,
13                        "CTXCAM ": false,
14                        "CTXGUSB": false
15                                    }
16
17                                   }
18
19          }
20
21      }
22
23  }
24
25
26  <!--NeedCopy-->
```

Lista de opciones de canal virtual, junto con sus descripciones:

- “CTXCPM”: Impresión PDF.
- “CTXCCM”: Asignación de puertos serie del cliente.
- “CTXCLIP”: Operaciones del portapapeles desde la sesión al VDA y desde el VDA a la sesión.
- “CTXCAM”: Asignación de sonido del cliente.
- “CTXMM”: Redirección multimedia de Citrix.
- “CTXCTL”: Canal virtual de control de Citrix.
- “CTXEUEM”: Supervisión de la experiencia del usuario final.
- “CTXGUSB”: Redirigir los dispositivos USB a la sesión.
- “CTXFILE”: La transferencia segura de archivos tiene lugar entre un dispositivo de usuario y una sesión de Citrix Virtual Apps and Desktops y Citrix DaaS (antes denominado Citrix Virtual Apps and Desktops Service). Puede cargar y descargar archivos desde y hacia una sesión y acceder a los datos.
- “CTXMTCH”: La función multitoque envía todos los gestos a la sesión virtual. La aplicación reacciona en función de los gestos que admite.
- “CTXSCRD”: Compatibilidad con tarjetas inteligentes.
- “CTXMOB”: canal virtual de Receiver para móviles.
- “CTXMTOP”: canal virtual de Microsoft Teams.
- “CTXIME”: editor de métodos de entrada.
- “CTXCSB”: redirección de contenido del explorador.

- “CTXCDM”: asignación de unidades del cliente.
- “CTXTUI”: interfaz de usuario transparente.

Canales virtuales personalizados

El Virtual Channel SDK para Chrome permite que las aplicaciones Chrome de terceros escriban canales virtuales personalizados. Estos canales se inicializan con las sesiones de escritorios y aplicaciones iniciadas con la aplicación Citrix Workspace o con el SDK de HDX para Chrome.

Además, el Virtual Channel SDK ofrece una forma fácil de escribir y recibir datos de la aplicación Chrome de terceros y de la aplicación y el escritorio.

Modo de configuración

Para configurar canales virtuales personalizados, utilice la directiva administrativa de Google para incluir lo siguiente.

```
{

    "settings": {

        "Value": {

            "settings_version": "1.0",
                "engine_settings": {

                    "customVC": [
                        {

                    "appId": "xyz",
                    "streamName": "abc"
                         }

                    ]
                 }

          }

      }

 }


<!--NeedCopy-->
```

Lista de opciones de CustomVC, junto con sus descripciones:

- “appId”: El ID de la aplicación de Chrome que implementa los canales virtuales personalizados.

- "streamName": El nombre del canal virtual.

Solucionar problemas técnicos

May 16, 2024

Cómo recopilar registros

La aplicación Citrix Workspace para ChromeOS proporciona marcas de hora en los registros generados por el dispositivo del usuario. La aplicación Citrix Workspace permite recopilar registros para sesiones en curso de aplicaciones y escritorios virtuales.

Como usuario final, puede recopilar registros para ayudar a solucionar problemas. Los registros se pueden generar tanto en el dispositivo del usuario como en las máquinas. Los registros pueden ser para escritorios y aplicaciones.

Antes, podía recopilar registros solo para las sesiones iniciadas después de seleccionar **Iniciar registro** durante una sesión en curso. Ahora, los registros se recopilan para las sesiones en curso y las siguientes hasta que seleccione **Detener registro**.

Para habilitar la captura de registros en los dispositivos de usuario

1. En el dispositivo del usuario, inicie la aplicación Citrix Workspace y vaya a la página de inicio de sesión.
2. Seleccione el botón con una imagen de parámetros en la esquina inferior derecha.
3. En el cuadro de diálogo **Parámetros**, haga clic en **Iniciar registro**.

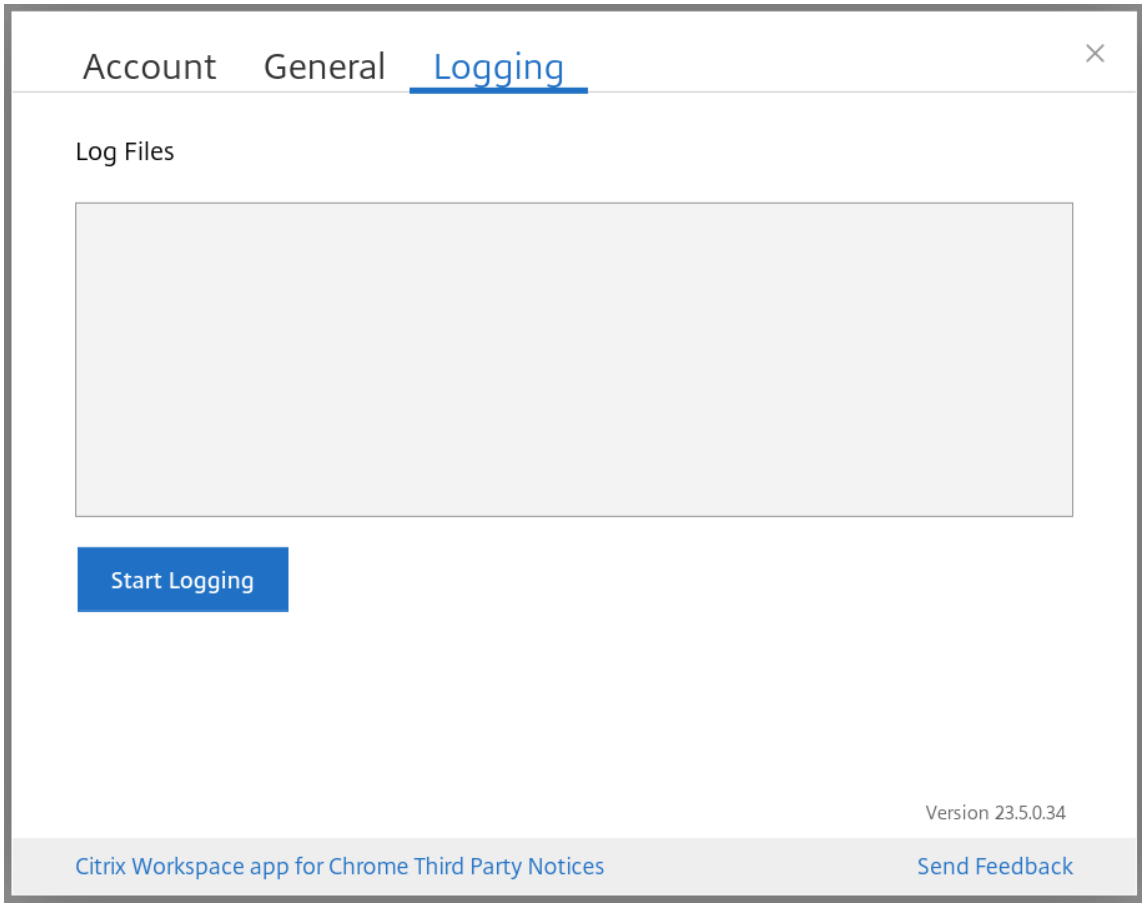
   A continuación, en el cuadro de diálogo **Parámetros**, aparece una lista de los archivos de registro recopilados.
4. Haga clic en **Detener registro** para finalizar la recopilación de los registros del dispositivo de usuario.

Registros del cliente

> **Nota:**
>
> - A partir de la versión 2207, los registros de la consola forman parte de los registros del cliente.

1. Haga clic en el botón **Parámetros** que hay en la parte inferior derecha de la pantalla **Iniciar sesión** de la aplicación Citrix Workspace.

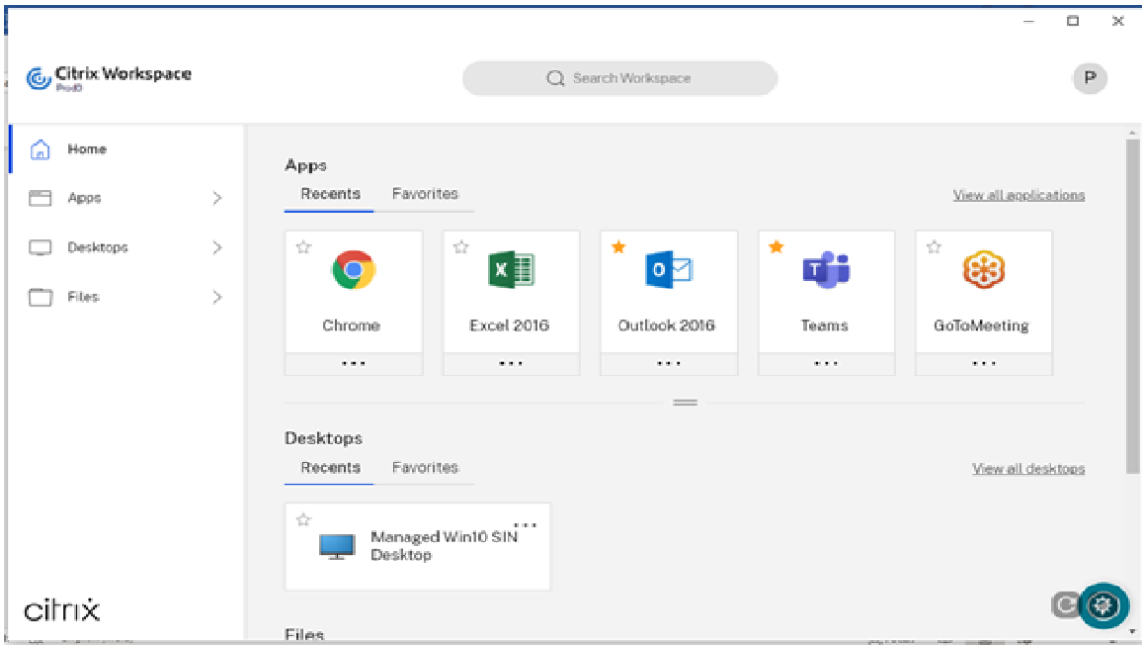
2. Haga clic en el botón **Iniciar registro** en **Registros** para habilitar la recopilación de registros.



3. El botón **Iniciar registro** cambia a **Detener registro**. Este cambio indica que la recopilación de registros está habilitada.

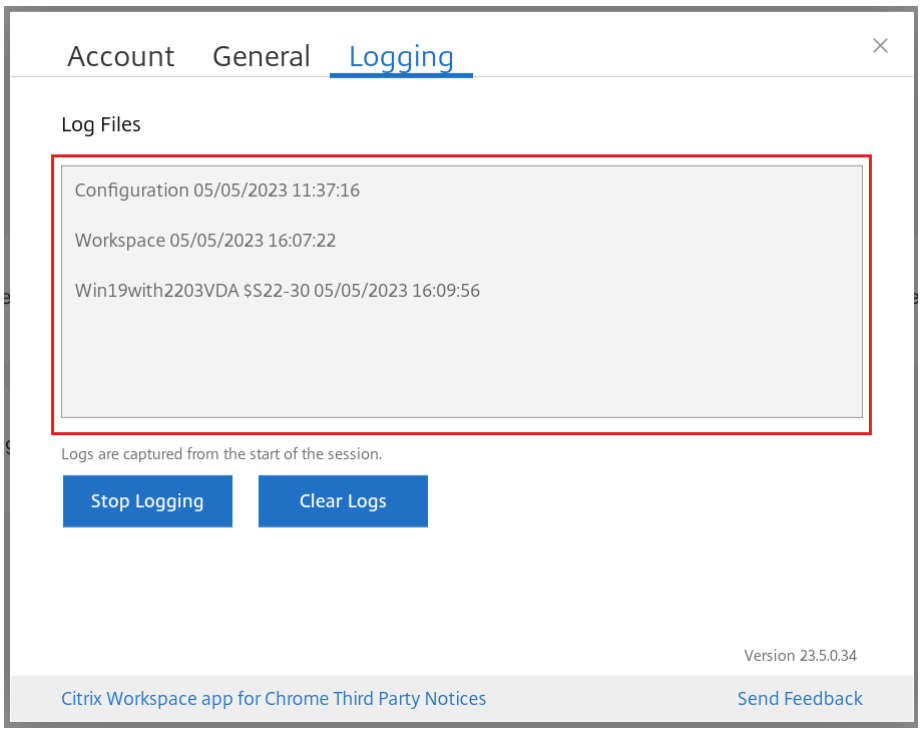
   Cierre el cuadro de diálogo **Cuenta**.

4. Inicie sesión en el escritorio virtual de la aplicación Citrix Workspace e inicie la sesión de su aplicación virtual y reproduzca el problema para recopilar registros.



   Continúe trabajando en la sesión para reproducir el problema.

5. Una vez que se haya reproducido el problema, cierre la sesión.
6. Haga clic de nuevo en el botón **Parámetros** para abrir el cuadro de diálogo **Cuenta**.
7. Seleccione la ficha **Captura de registros**.
8. El cuadro de diálogo **Registros** muestra la lista de **archivos de registros** capturados.



9. Al pasar el mouse encima de los archivos de registros, se muestra una pequeña flecha a la derecha.

10. Haga clic en el botón de la flecha para descargar y guardar el archivo de registros.
11. Guarde todos los archivos de registro indicados en **Archivos de registros** y compártalos con el administrador o el ingeniero de asistencia de Citrix.
12. Haga clic en **Detener registro**.

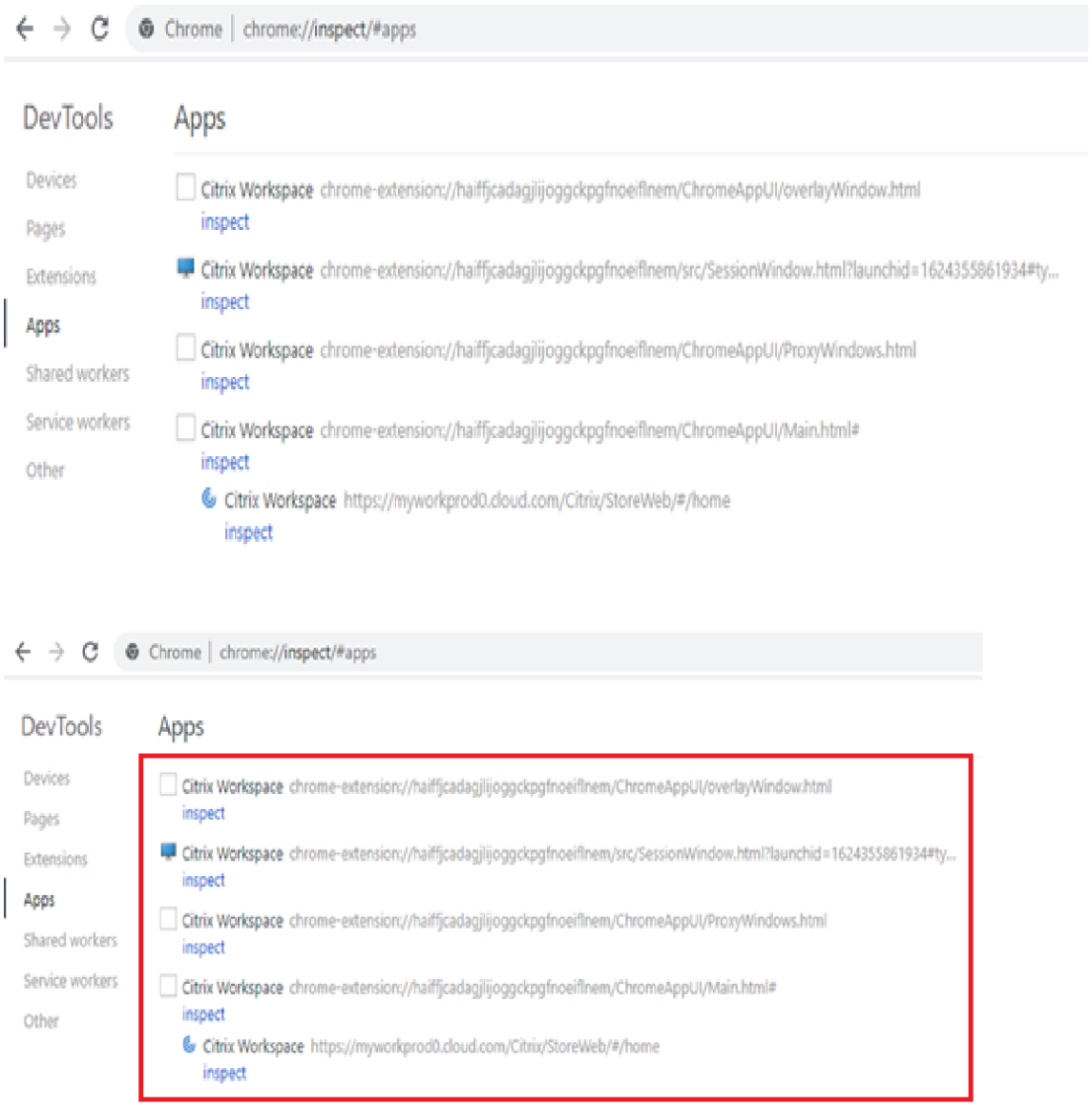
> **Nota:**
>
> En modo quiosco, los archivos se pueden guardar en un dispositivo USB extraíble.

Registros de la consola

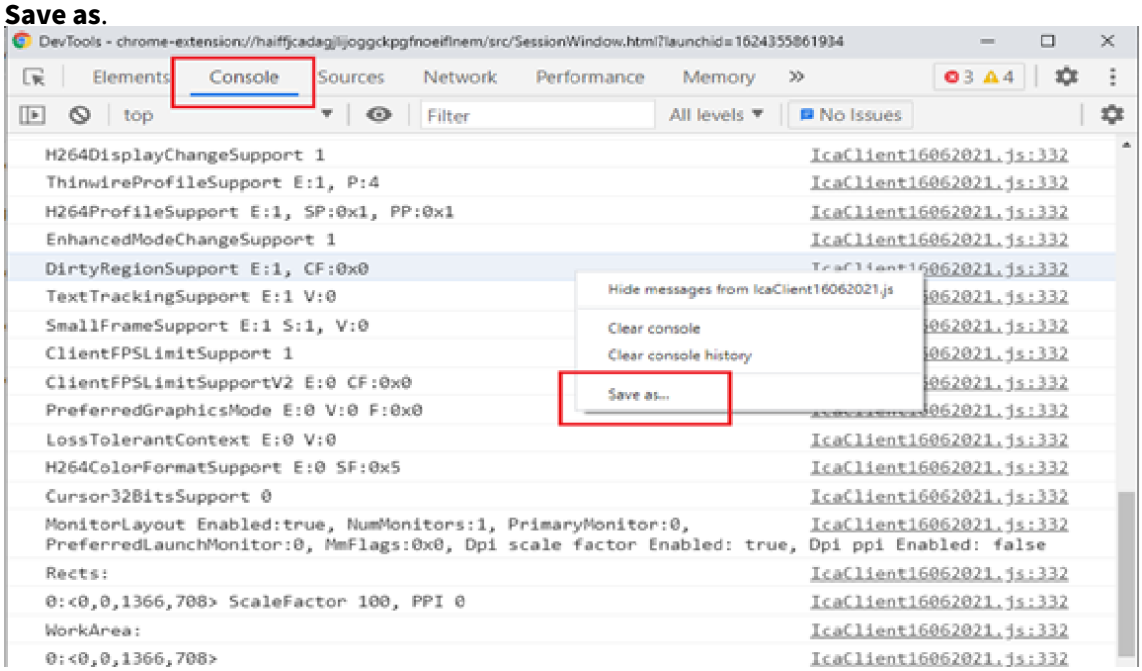
Nota:

- A partir de la versión 2207, los registros de la consola forman parte de los registros del cliente. Por lo tanto, ahora basta con recopilar los registros del cliente.

1. Abra la página **chrome://inspect/#apps** en el explorador Google Chrome de la aplicación Citrix Workspace.
2. En la ficha **Apps**, haga clic en **Inspect** en todas las ventanas relacionadas con Citrix Workspace: SessionWindow.html, Main.html (y sus nodos secundarios).



3. Para cada ventana de herramienta para desarrolladores abierta, haga clic en **Console**. A continuación, para guardar todo el registro, haga clic con el botón secundario y seleccione la opción **Save as**.



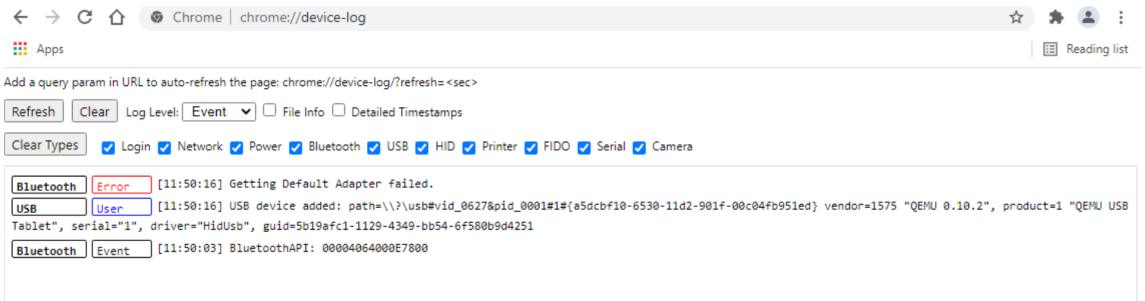
Registros de redirección USB

1. Siga los pasos que se indican en Mediante web.config para ChromeOS y habilite moreLogs para USB de la siguiente manera:

   Agregue el valor de configuración de moreLogs a chromeAppPreferences en el archivo web.config de StoreFront:

   ```
   chromeAppPreferences ='{ "moreLogs":{ "usb":true } } '
   ```

2. A continuación, abra una nueva ficha en el explorador Google Chrome e introduzca **chrome://device-log** y comparta los registros.



Registros de transferencias de archivos

Los registros de transferencia de archivos se pueden obtener desde el cliente y desde el servidor.

Para obtener registros de transferencia de archivos desde el cliente:

1. Abra un explorador web.
2. Vaya a la siguiente dirección URL para iniciar la captura de registros:
   <storefronturl>/clients/html5client/src/viewlog.html
   donde <*storefronturl*> es el FQDN o dirección IP del servidor de StoreFront donde está configurado el almacén.

Para obtener más información sobre la transferencia de archivos, consulte Transferencia de archivos en HTML5 y Chrome.

Registros de la optimización de Microsoft Teams

La optimización de Microsoft Teams admite la versión más reciente, 1.8.0.12, de la biblioteca de correcciones de compatibilidad.

Para saber la versión actual de la biblioteca de correcciones de compatibilidad que utiliza:

1. Inicie la aplicación Microsoft Teams e inicie una llamada con uno de los usuarios.
2. Maximice la ventana de Microsoft Teams después de que se haya establecido la llamada.
3. Abra el **teclado en pantalla** dentro de la sesión y haga clic en las teclas **Ctrl + Alt + Mayús + 1**. Ahora puede ver los archivos de registros en la carpeta de descargas.
4. Abra el archivo `MSTeams Diagnostics Log <date><time>_vdi partner.txt` y busque la versión de la biblioteca en **type_script**.
   Compare la versión de la biblioteca con 1.8.0.12.
5. (Opcional) Si la versión de la biblioteca no es 1.8.0.12, contacte con el administrador para actualizarla a la versión más reciente.

Registros del cliente en modo quiosco

Para recopilar los registros en modo quiosco:

1. Conecte un dispositivo USB extraíble a su Chromebook.
2. Descargue el archivo de registros.
3. Guarde el archivo de registros en el dispositivo USB conectado.

   El archivo de registros se transfiere al dispositivo USB.

Accesos directos

- Es posible que el atajo de teclado Ctrl + Alt + Mayús + 1 no funcione en Microsoft Teams optimizado dentro de un escritorio virtual. Como solución temporal, abra el **teclado en pantalla** y use el atajo. [RFHTMCRM-5441]

Herramienta de la utilidad de configuración

May 16, 2024

Existen cuatro opciones para personalizar la aplicación Citrix Workspace para ChromeOS:

- configuration.js
- web.config
- default.ica
- Directiva de Google

Las cuatro opciones están disponibles en la utilidad de configuración, que es una página web de configuración basada en la interfaz de usuario.

Descargue la Herramienta de la utilidad de configuración de la página Descargas.

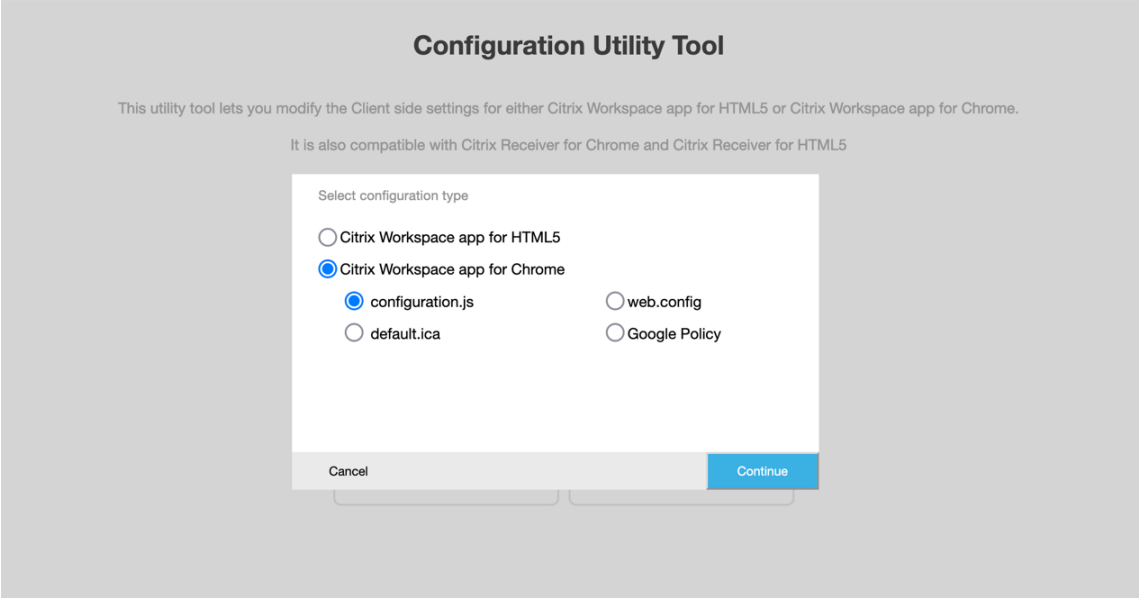
Cómo usar la herramienta de la utilidad de configuración

1. Haga clic en **Create New.**
2. Seleccione **Citrix Workspace app for Chrome** y elija una de las cuatro opciones de configuración. A continuación, haga clic en **Continue** para continuar o en **Cancel** para volver a la página principal.

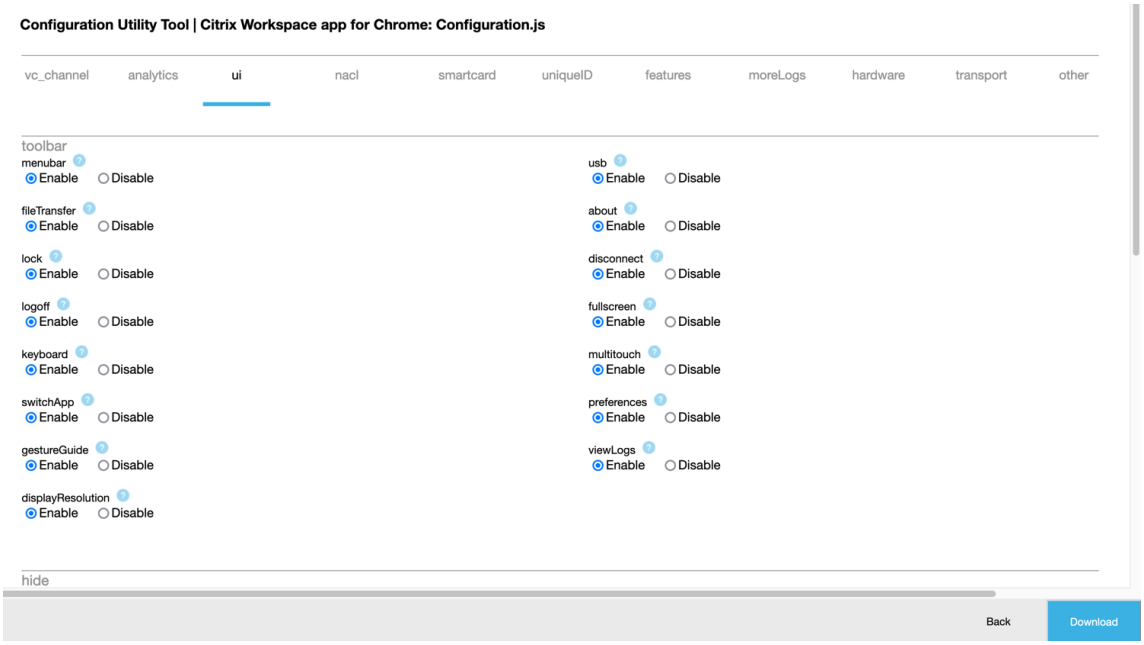
Para configuration.js

Para crear una configuración:

1. Después de seleccionar **configuration.js**, haga clic en **Continue** para seguir con la configuración o en **Cancel** para volver a la página principal.



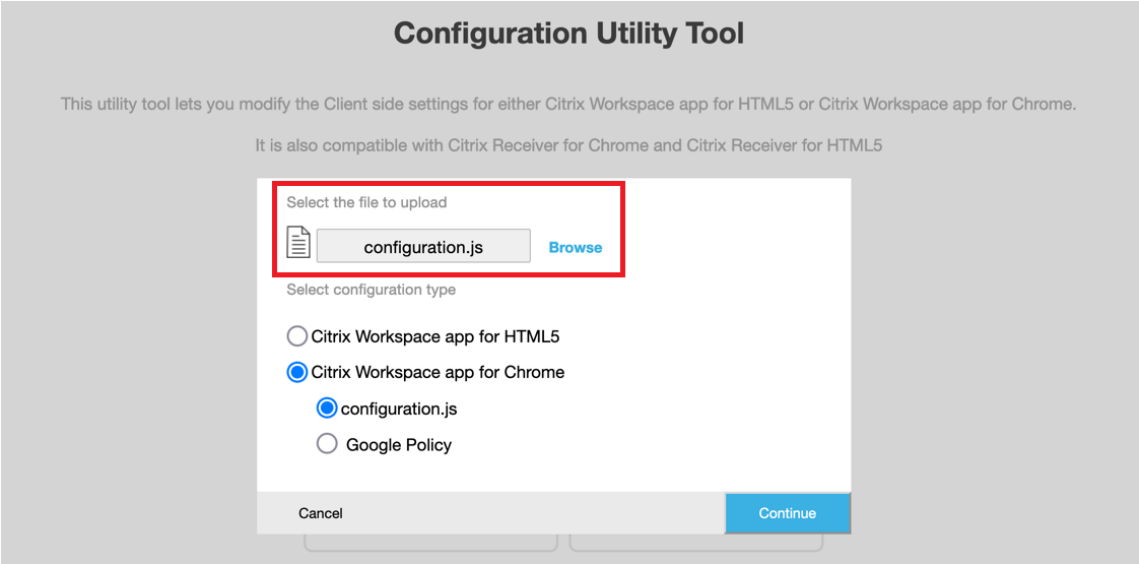
2. En la **herramienta de la utilidad de configuración**, seleccione las funciones que quiera y elija sus valores correspondientes.



3. Haga clic en **Download** para descargar el archivo configuration.js.

Para modificar una configuración:

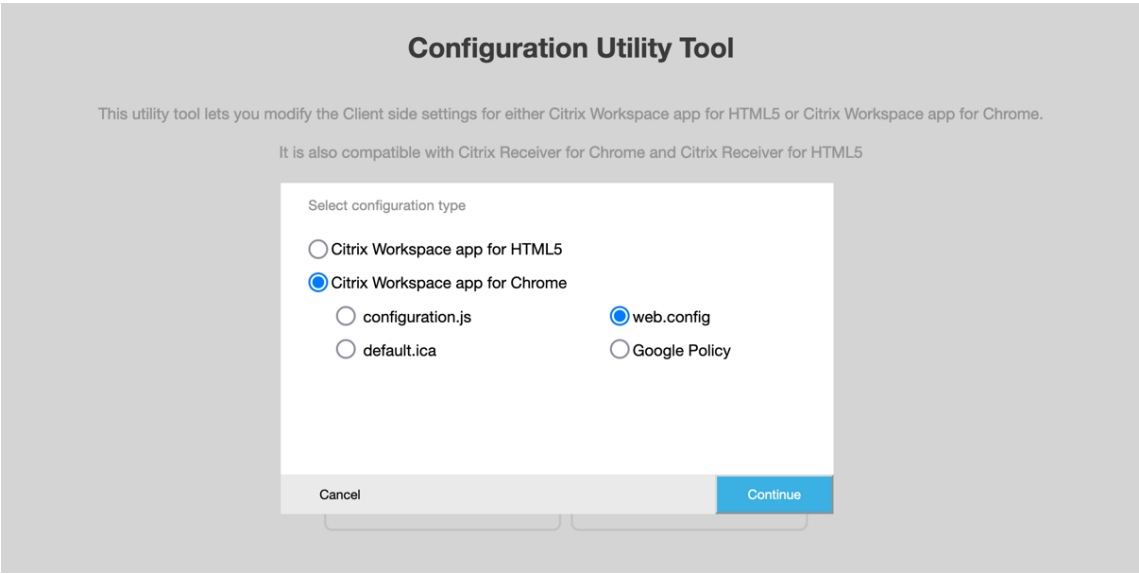
1. Haga clic en **Upload existing file**.
2. Seleccione **Citrix Workspace app for Chrome** y seleccione **configuration.js**.
3. Haga clic en **Browse** y vaya a la ubicación del archivo configuration.js para seleccionar el archivo y cargarlo.



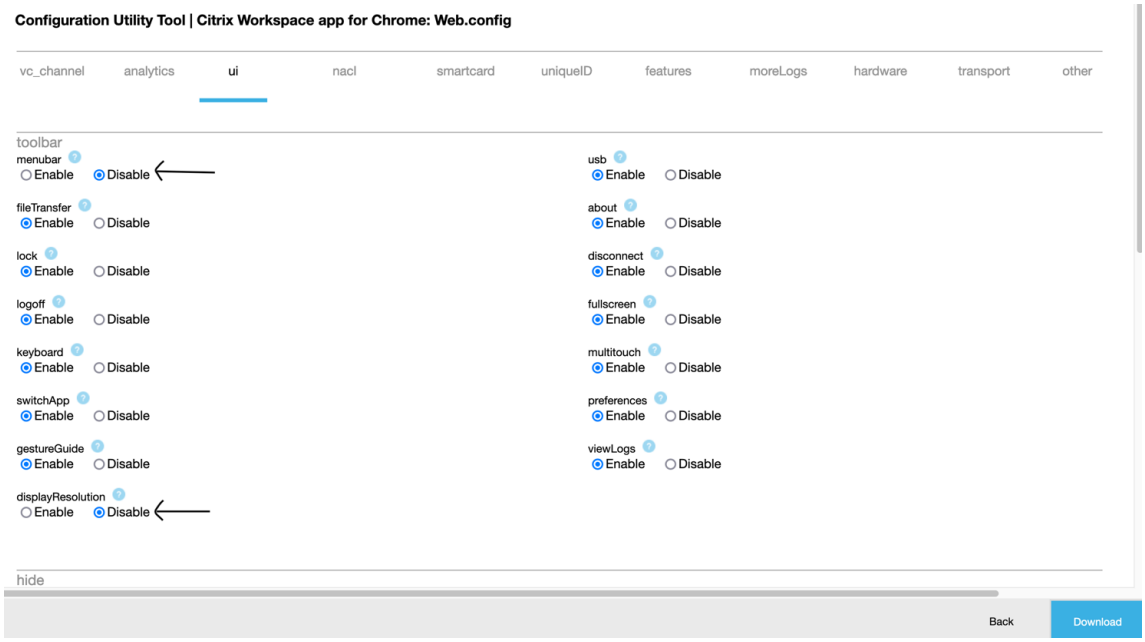
4. Haga clic en **Continue** para seguir con la configuración o en **Cancel** para volver a la página principal.
5. Seleccione las funciones que quiera y elija sus valores correspondientes.
6. Haga clic en **Download** para descargar el archivo configuration.js.

Para web.config (en StoreFront)

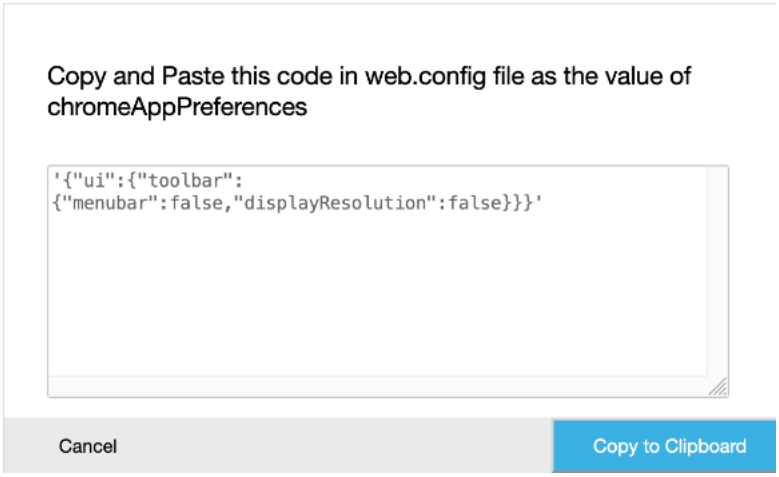
1. Después de seleccionar **web.config**, haga clic en **Continue** para seguir con la configuración o en **Cancel** para volver a la página principal.



2. Seleccione los parámetros que quiera y sus valores correspondientes y haga clic en **Descargar** (por ejemplo, seleccione menubar: inhabilitar; displayResolution: inhabilitar)



3. Copie el contenido del cuadro de diálogo.



4. Abra el archivo web.config del sitio de Citrix Receiver para Web. Este archivo se encuentra en **C:\inetpub\wwwroot\Citrix\storenameWeb**, donde "storename"es el nombre que se especificó para el almacén cuando se creó.
5. Busque el campo chromeAppPreferences en el archivo y defina su valor con la cadena JSON copiada del cuadro de diálogo.

```
chromeAppPreferences = '{

    "ui":{

        "toolbar":{

            "menubar":false,"displayResolution":false
             }
```



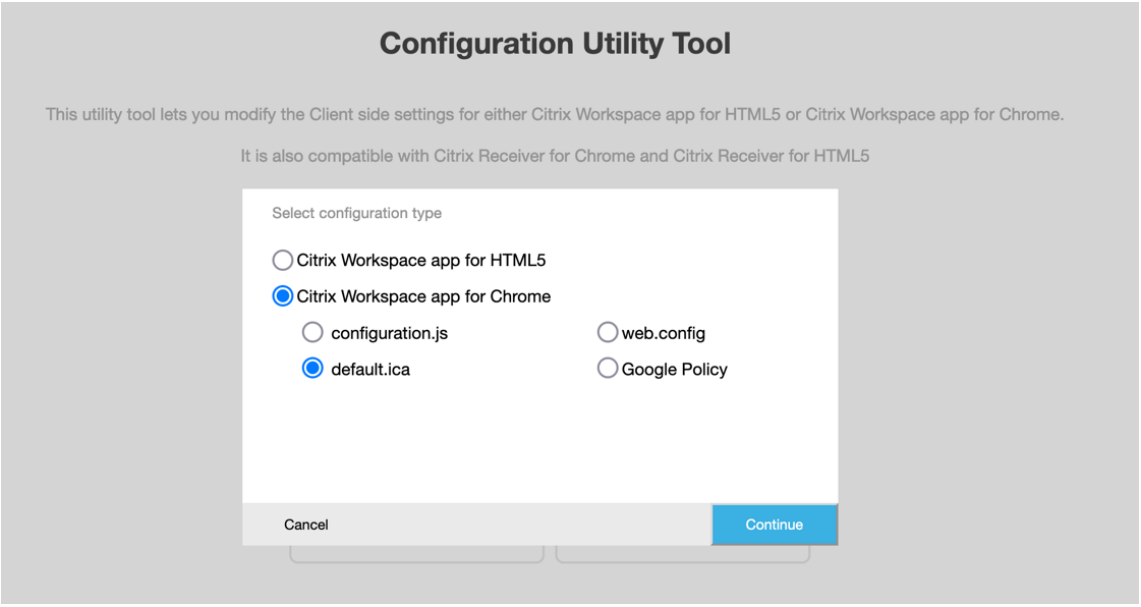
```
                        }

                        }
 '
<!--NeedCopy-->
```

web.config default.ica

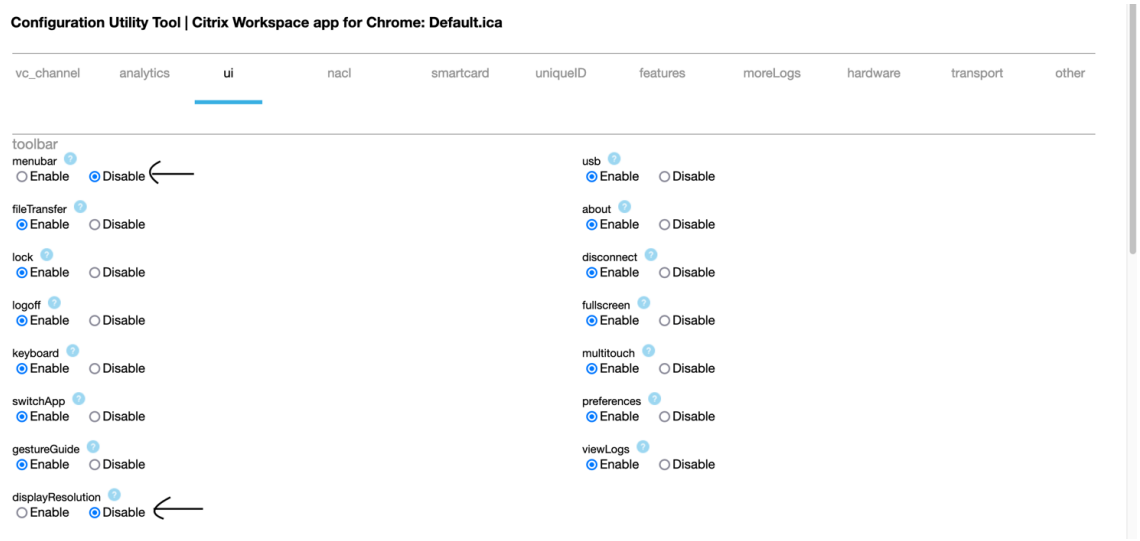
```
    <csrfProtection excludedUserAgents="CitrixReceiver;CitrixWebAPI-NoCSRFToken" />
  </serverSettings>
  <clientSettings>
    <authManager getUsernameURL="Authentication/GetUserName" logoffURL="Authentication/Logoff"
      changeCredentialsURL="ExplicitAuth/GetChangeCredentialForm"
      loginFormTimeout="5" webviewReturnURL="ExplicitAuth/Bounce"
      webviewResumeURL="ExplicitAuth/ResumeForms" allowSelfServiceAccountManagementURL="ExplicitAuth
    <storeProxy keepAliveURL="Home/KeepAlive">
      <resourcesProxy listURL="Resources/List" resourceDetails="default" />
      <sessionsProxy listAvailableURL="Sessions/ListAvailable" disconnectURL="Sessions/Disconnect"
        logoffURL="Sessions/Logoff" />
      <clientAssistantProxy getDetectionTicketURL="ClientAssistant/GetDetectionTicket"
        getDetectionStatusURL="ClientAssistant/GetDetectionStatus" />
    </storeProxy>
    <pluginAssistant enabled="true" upgradeAtLogin="false" showAfterLogin="false">
      <win32 path="http://downloadplugins.citrix.com/Windows/CitrixReceiverWeb.exe" />
      <macOS path="http://downloadplugins.citrix.com/Mac/CitrixReceiverWeb.dmg"
        minimumSupportedOSVersion="10.6" />
      <html5 enabled="Fallback" platforms="Firefox;Chrome;Version/([6-9]|\d\d).*Safari;MSIE \d\d;Tri
        launchURL="clients/HTML5Client/src/SessionWindow.html" preferences=""
        singleTabLaunch="false" chromeAppOrigins="chrome-extension://haiffjcadagjlijoggckpgfnoeiflne
        chromeAppPreferences = '{"ui":{"toolbar":{"menubar":false,"displayResolution":false}}}' />
      <protocolHandler enabled="true" platforms="(Macintosh|Windows NT).*((Firefox/((5[2-9]|[6789][0
        skipDoubleHopCheckWhenDisabled="false" />
    </pluginAssistant>
```

Para default.ica

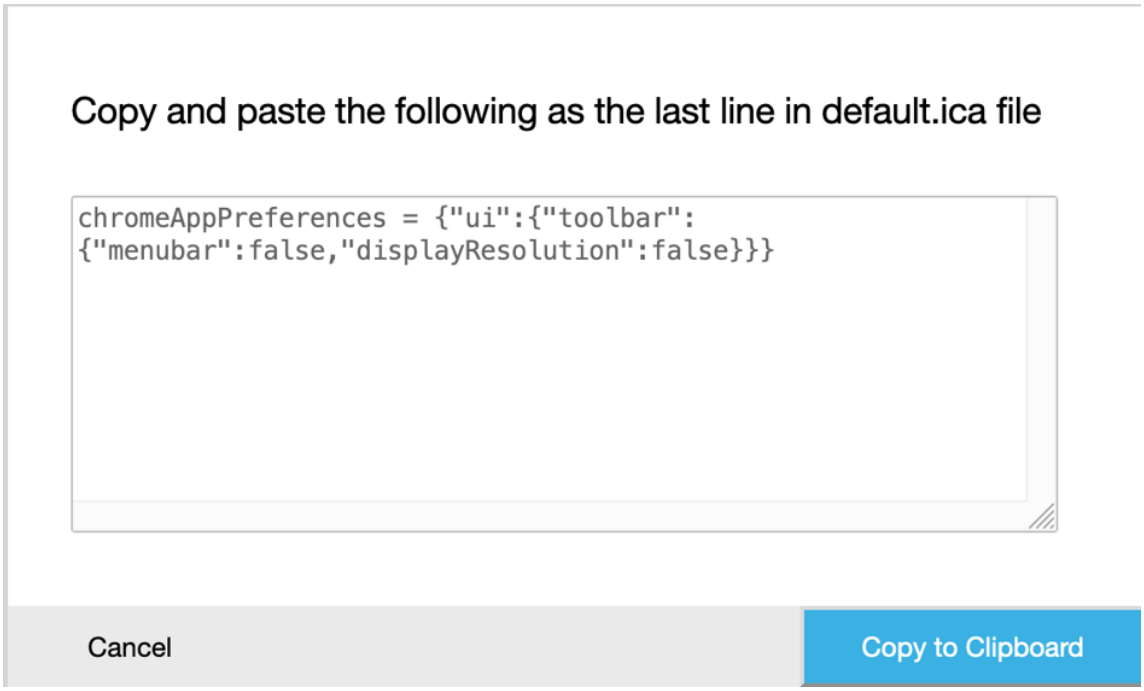
1. Después de seleccionar **default.ica**, haga clic en **Continue** para seguir con la configuración o en **Cancel** para volver a la página principal.



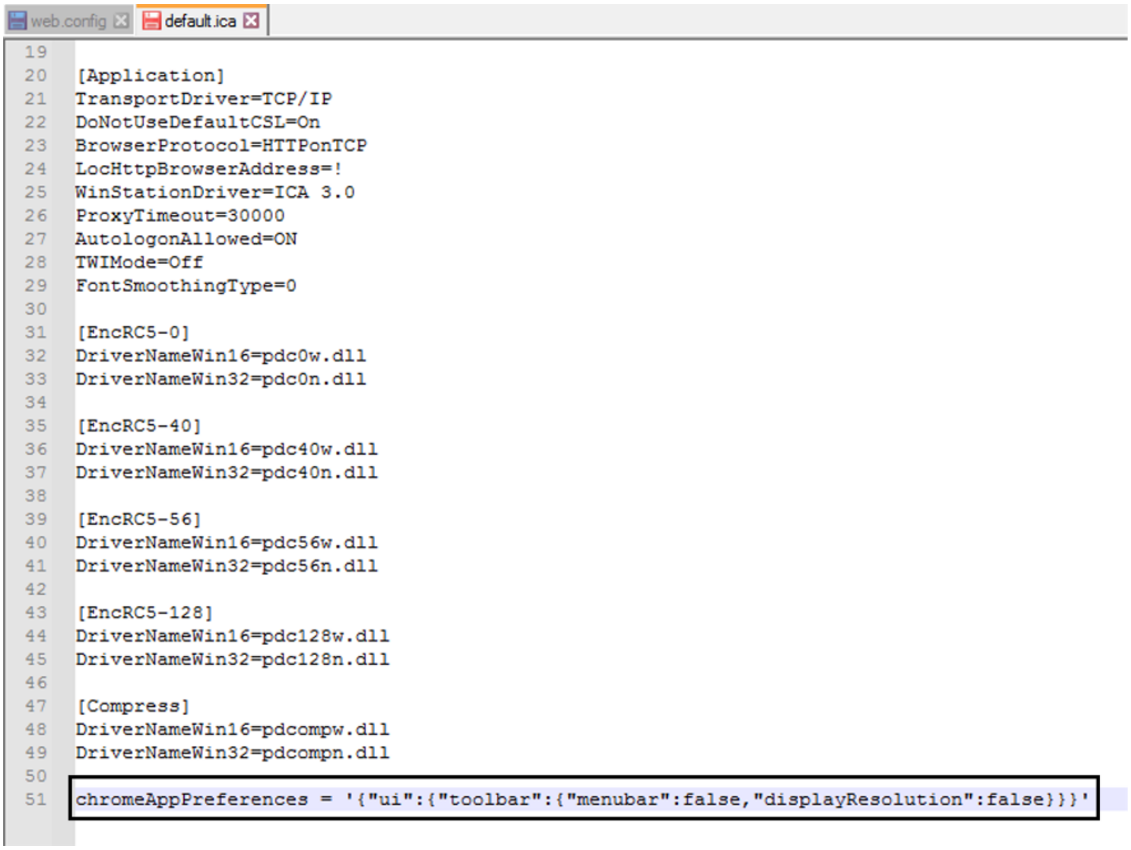
2. Seleccione los parámetros que quiera y sus valores correspondientes y haga clic en **Descargar** (por ejemplo, seleccione **menubar** > **inhabilitar** y **displayResolution** > **inhabilitar**).



3. Copie el contenido del cuadro de diálogo.



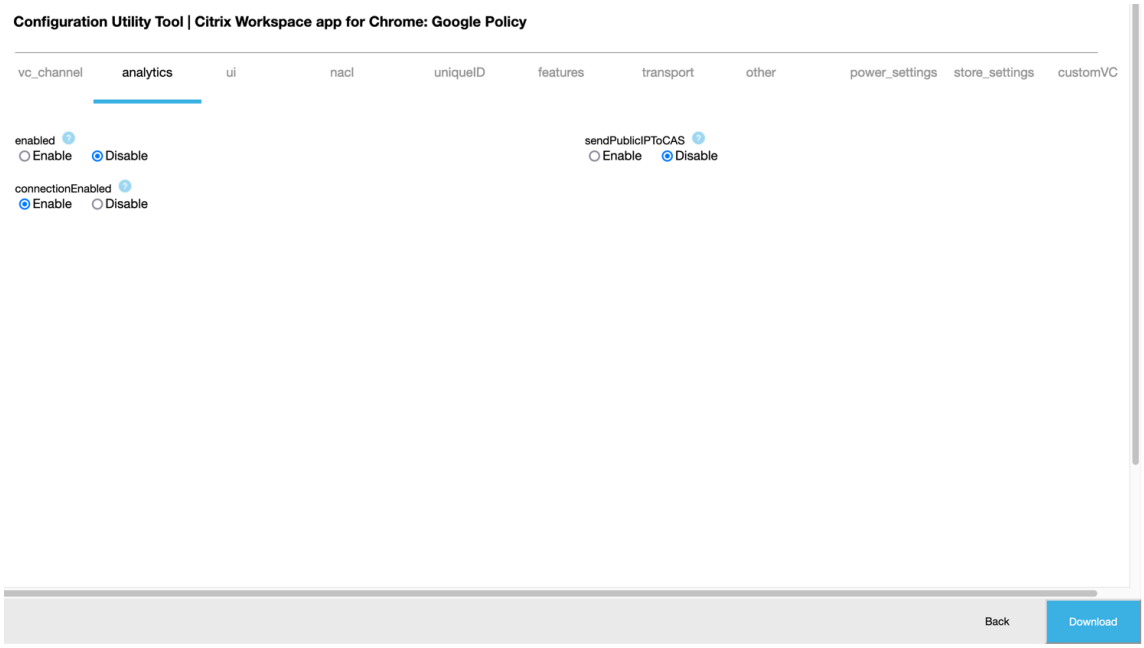
4. Abra el archivo default.ica, que normalmente se halla en **C:\inetpub\wwwroot\Citrix\<nombre del sitio>\conf\default.ica** para los clientes de la Interfaz Web, donde "nombre del sitio"es el nombre especificado para el sitio cuando se creó. Para los clientes de StoreFront, el archivo default.ica suele hallarse en **C:\inetpub\wwwroot\Citrix\<Storename>\App_Data\default.ica**, donde "Storename"es el nombre que se especificó para el almacén cuando se creó.
5. Agregue el contenido de la última línea del archivo default.ica como se indica aquí.



Para la directiva de Google

Cómo crear una configuración

1. Después de seleccionar **Google Policy**, haga clic en **Continue** para seguir con la configuración o en **Cancel** para volver a la página principal.
2. Seleccione los parámetros pertinentes y sus valores correspondientes, y haga clic en **Download** (por ejemplo, seleccione sendPublicIPToCas: disabled)

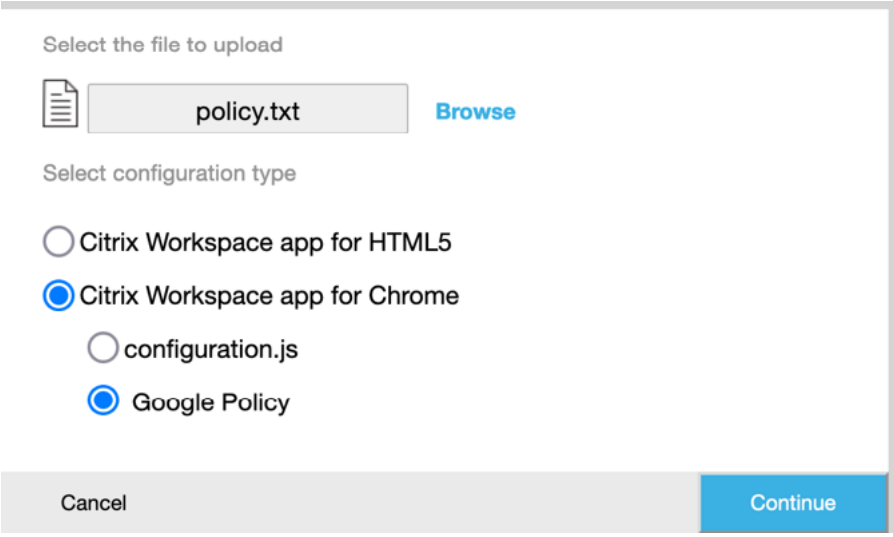


3. Al hacer clic en **Download**, se crea un archivo **policy.txt**.

Cómo modificar una configuración

> **Limitación de la función:**
>
> Solo puede modificar los parámetros y los valores que están presentes en el archivo de carga (**policy.txt**). Si necesita modificar otras directivas, cree un archivo de directivas para incluir los parámetros. Para obtener más información, consulte Cómo crear una configuración.

1. Haga clic en **Upload existing file**.
2. Seleccione **Citrix Workspace app for Chrome** y seleccione **policy.txt**.



3. Haga clic en **Browse** y vaya a la ubicación del archivo **policy.txt** para seleccionar y cargar el archivo.
4. Haga clic en **Continue** para seguir con la modificación o en **Cancel** para volver a la página principal.
5. Para modificar los parámetros, elija los valores correspondientes.
6. Haga clic en **Download** para descargar el archivo **policy.txt** actualizado.

Autenticación

June 18, 2024

Tarjeta inteligente

La aplicación Citrix Workspace para ChromeOS admite lectores de tarjetas inteligentes USB con StoreFront. Puede usar tarjetas inteligentes con estos fines:

- Autenticación del inicio de sesión con tarjetas inteligentes en la aplicación Citrix Workspace.
- Aplicaciones publicadas para acceder a dispositivos locales de tarjeta inteligente.
- Tarjetas inteligentes para firmar documentos y correos electrónicos. Por ejemplo, Microsoft Word y Outlook que se inician en sesiones ICA.

Las tarjetas inteligentes compatibles (con lectores de tarjetas inteligentes USB) incluyen:

- Personal Identity Verification (PIV)
- Tarjetas CAC (Common Access Card)

Requisitos previos

- Versión 3.6 de StoreFront o una posterior
- XenDesktop 7.6 o versiones posteriores
- XenApp 6.5 o versiones posteriores
- Citrix Virtual Apps and Desktops 1808 o versiones posteriores
- Aplicación Citrix Workspace 1808 o versiones posteriores

> **Importante:**
>
> - Para la autenticación con tarjeta inteligente en StoreFront 3.5 y versiones anteriores, necesita un script personalizado para habilitar la autenticación con tarjeta inteligente. Contacte con Citrix Support para obtener ayuda.
> - Para acceder a la información más reciente sobre las versiones compatibles, consulte los hitos del ciclo de vida de la aplicación Citrix Workspace y Citrix Virtual Apps and Desktops.

Requisitos previos para la configuración de dispositivos

- Google Smart Card Connector es una aplicación que interactúa con los lectores de tarjetas inteligentes USB del dispositivo. La aplicación conectora expone las API de Personal Computer Smart Card (PCSC) Lite a otras aplicaciones, incluida la aplicación Citrix Workspace.
- Los proveedores de certificados son las aplicaciones de middleware escritas por proveedores que interactúan con el conector de tarjetas inteligentes. Las aplicaciones de middleware acceden al lector de tarjetas inteligentes, leen certificados y proporcionan certificados de tarjetas inteligentes a ChromeOS.

  Las aplicaciones de middleware también implementan una funcionalidad de firma mediante solicitudes de PIN.
  Por ejemplo, CACKey.

  Para obtener más información, consulte Deploy smart cards on ChromeOS.
- Al configurar la autenticación con tarjetas inteligentes en StoreFront, la aplicación Citrix Workspace solicita a ChromeOS que proporcione certificados del cliente en la tarjeta inteligente. ChromeOS presenta los certificados tal y como los recibe de los proveedores. Las solicitudes de PIN hacen referencia a la autenticación.

  La aplicación Citrix Workspace tiene una lista aprobada de sistemas operativos permitidos para la autenticación con tarjetas inteligentes. StoreFront 3.6 y versiones posteriores también aprueban ChromeOS. Para versiones anteriores de StoreFront, puede usar un script personalizado para permitir la autenticación con tarjetas inteligentes en ChromeOS. Contacte con la asistencia de Citrix para obtener scripts personalizados.

- La aplicación Citrix Workspace no controla el flujo de trabajo de la autenticación con tarjetas inteligentes con StoreFront. Sin embargo, en algunos casos, StoreFront puede solicitarle que cierre el explorador web para borrar las cookies.

  Para borrar todas las cookies y cargar de nuevo la URL del almacén, haga clic en el botón de recarga de la aplicación Citrix Workspace para ChromeOS.

  En ocasiones, para borrar las cookies, puede cerrar sesión en el dispositivo ChromeOS.

- Al intentar iniciar una sesión de aplicación o escritorio, la aplicación Citrix Workspace no usa la redirección de tarjetas inteligentes. En su lugar, interactúa con la aplicación conectora de tarjetas inteligentes para las API de PC/SC lite.

  Las solicitudes de PIN necesarias para iniciar sesión en Windows aparecen en la sesión. En este caso, los proveedores de certificados no tienen ningún rol. La aplicación Citrix Workspace administra las actividades de la sesión, como el doble salto o la firma de correos electrónicos.

Limitaciones de las tarjetas inteligentes

- Al extraer la tarjeta inteligente del dispositivo ChromeOS, el certificado de la tarjeta inteligente se almacena en la caché. Este comportamiento es un problema conocido de Google Chrome. Reinicie el dispositivo ChromeOS para borrar la caché.
- Al reempaquetar la aplicación Citrix Workspace para ChromeOS, como administrador, obtenga la aprobación de appID por parte de Google. Con ello, se confirma que la aplicación conectora de tarjetas inteligentes puede acceder.
- Solo se admite un lector de tarjeta inteligente a la vez.
- No se admiten tarjetas inteligentes virtuales ni tarjetas inteligentes rápidas.
- Las tarjetas inteligentes no se admiten en Citrix Workspace (nube).

Para configurar la compatibilidad con tarjetas inteligentes en el dispositivo ChromeOS

1. Instale la aplicación de conector de tarjeta inteligente. La aplicación de tarjeta inteligente es necesaria para la compatibilidad con Personal Computer Smart Card (PCSC) en el dispositivo ChromeOS. Esta aplicación lee la tarjeta inteligente mediante la interfaz USB. Esta aplicación puede instalarse desde el sitio Web de Chrome.
2. Instale la aplicación de middleware. Se necesita una aplicación de middleware como interfaz que se comunique con la tarjeta inteligente y los demás certificados de cliente. Por ejemplo, Charismathics o CACKey:

   - Para instalar la extensión de tarjeta inteligente de Charismathics o CACKey, consulte las instrucciones descritas en el sitio web de Chrome.

- Para obtener más información sobre las aplicaciones de middleware y la autenticación con tarjeta inteligente, consulte el sitio de asistencia técnica de Google.

3. Configure la autenticación con tarjeta inteligente mediante:

   - Citrix Gateway
   - Consola de administración de StoreFront

   Para obtener información, consulte Configuring Smart Card Authentication y Configurar el servicio de autenticación en la documentación de Citrix Gateway.

Autenticación SAML

Para configurar Single Sign-On:

1. Configure el proveedor de identidades (IdP) de terceros para la autenticación SAML si todavía no lo tiene configurado. Por ejemplo, ADFS 2.0.

   Para obtener más información, consulte el artículo de Knowledge Center CTX133919.

2. Configure Single Sign-On con Google Apps mediante el proveedor de identidades de SAML. La configuración permite a los usuarios aplicar una identidad de terceros para usar aplicaciones de Google en lugar de la cuenta de Google Enterprise.

   Para obtener más información, consulte Set-up single sign-on for managed Google Accounts using third-party Identity providers en la asistencia técnica de Google.

3. Configure los dispositivos Chrome para que inicien sesión a través del IdP de SAML. La configuración permite a los usuarios iniciar sesión en dispositivos Chrome con un proveedor de identidad de terceros.

   Para obtener más información, consulte Configure SAML Single Sign-On for Chrome devices en Google Support.

4. Configure Citrix Gateway para que inicie sesión a través del IdP de SAML. La configuración permite a los usuarios iniciar sesión en Citrix Gateway mediante un proveedor de identidades de terceros.

   Para obtener más información, consulte Configuración de la autenticación SAML.

5. Configure Citrix Virtual Apps and Desktops para la autenticación federada con el fin iniciar sesión en sesiones de Citrix Virtual Apps and Desktops mediante certificados generados dinámicamente. Puede hacerlo después del proceso de inicio de sesión de SAML en lugar de escribir las combinaciones de nombre de usuario y contraseña.

   Para obtener más información, consulte Servicio de autenticación federada.

Para lograr el SSO para aplicaciones y escritorios virtuales, debe implementar un Servicio de autenticación federada (FAS).

> **Nota:**
>
> Sin FAS, se le pedirán el nombre de usuario y la contraseña de Active Directory. Para obtener más información, consulte Habilitar Single Sign-On para espacios de trabajo con el Servicio de autenticación federada de Citrix.

6. Instale y configure la extensión SAML SSO para la aplicación Chrome en los dispositivos Chrome. Para obtener más información, consulte este sitio web de Google. Esta extensión obtiene cookies de SAML del explorador web y las suministra la aplicación Citrix Workspace. Esta extensión tiene que estar configurada con la siguiente directiva para permitir que Citrix Workspace obtenga las cookies de SAML:

   Si reempaqueta la aplicación Citrix Workspace para ChromeOS, cambie el valor de appId correctamente. Luego, cambie el dominio por el dominio del proveedor de identidades de SAML de su empresa.

```
{

    "whitelist" : {

        "Value" : [
            {

            "appId" : "haiffjcadagjlijoggckpgfnoeiflnem",
            "domain" : "saml.yourcompany.com"
             }

        ]
      }

 }

<!--NeedCopy-->
```

7. Configure Citrix Workspace para usar Citrix Gateway configurado para el inicio de sesión SAML. La configuración permite a los usuarios usar Citrix Gateway configurado para el inicio de sesión SAML. Para obtener más información sobre la configuración de ChromeOS, consulte el artículo CTX141844 de Knowledge Center.

Single Sign-on en la aplicación Citrix Workspace con Okta como proveedor de identidades

May 16, 2024

Puede configurar el Single Sign-On (SSO) en la aplicación Citrix Workspace con Okta como proveedor de identidades (IdP).

Requisitos previos

Los siguientes requisitos previos requieren privilegios de administrador:

- Citrix Cloud
- Cloud Connectors

  > **Nota:**
  >
  > Si es la primera vez que usa Citrix Cloud, defina una ubicación de recursos y configure los conectores. Se recomienda tener al menos dos Cloud Connectors implementados en entornos de producción. Para obtener información sobre la instalación de Citrix Cloud Connector, consulte Instalación de Cloud Connector.

- Aplicación Citrix Workspace
- Servicio de autenticación federada (opcional). Para obtener más información, consulte Habilitar Single Sign-On para espacios de trabajo con el Servicio de autenticación federada de Citrix.
- Citrix DaaS (antes denominado Citrix Virtual Apps and Desktops Service)
- VDA unido al dominio de AD o dispositivos físicos unidos a AD
- Arrendatario de Okta
- Agente de autenticación de Windows integrada (IWA) para Okta
- Okta Verify (Okta Verify se puede descargar de la tienda de aplicaciones) (opcional)
- Active Directory (AD)

Cómo configurar el SSO

A continuación se indican los pasos para configurar el SSO para la aplicación Citrix Workspace con Okta como proveedor de identidades:

1. Instalar el agente de Okta AD

2. Crear una integración de aplicación web OIDC de Okta
3. Configurar la aplicación web OIDC de Okta
4. Crear un token de API de Okta
5. Conectar Citrix Cloud con su organización de Okta
6. Habilitar la autenticación con Okta para espacios de trabajo
7. Configurar la derivación de la autenticación de varios factores (MFA) de Okta
8. Configurar el agente IWA de Okta
9. Configurar la regla de redirección de IdP
10. Configurar IdP Okta con la consola de administración de Google
11. Configurar el SSO para la aplicación Citrix Workspace para ChromeOS con la extensión de Chrome SAML SSO

Instalar el agente de Okta AD

Requisitos previos:

Antes de instalar el agente, asegúrese de cumplir los requisitos previos mencionados en el enlace Active Directory integration prerequisites.

Para instalar el agente AD para Okta:

1. En el portal de administración de Okta, haga clic en **Directory** > **Directory Integrations**.
2. Haga clic en **Add Directory** > **Add Active Directory**.
3. Revise los requisitos de instalación siguiendo el flujo de trabajo, que cubre los requisitos de instalación y arquitectura del agente.
4. Haga clic en el botón **Set Up Active Directory** y, a continuación, en **Download Agent**.
5. Instale el agente de AD para Okta en un Windows Server. Para ello, siga las instrucciones que se indican en Install the Okta Active Directory agent.

Crear una integración de aplicación web OIDC de Okta

Para usar Okta como IdP, se debe crear una aplicación web **OIDC - OpenID Connect** de Okta para poder usar las credenciales de usuario con Citrix Cloud. Esta aplicación inicia la secuencia de inicio de sesión y también gestiona la redirección a la URL de Citrix Workspace en caso de que cierre sesión.

Para obtener más información, consulte Create an Okta OIDC web app integration.

Configurar la aplicación web OIDC de Okta

Una vez creada la aplicación OIDC de Okta, configúrela con los parámetros necesarios para Citrix Cloud. Estos parámetros son necesarios para fines de autenticación cuando los suscriptores inician sesión en Citrix Workspace con Okta.

Para obtener más información, consulte el enlace Configurar la aplicación web OIDC de Okta.

Crear un token de API de Okta

Para obtener más información sobre cómo crear un token de API de Okta, consulte Create an Okta API token.

Conectar Citrix Cloud con su organización de Okta

Para obtener más información sobre cómo conectar Citrix Cloud, consulte Connect Citrix Cloud to your Okta organization.

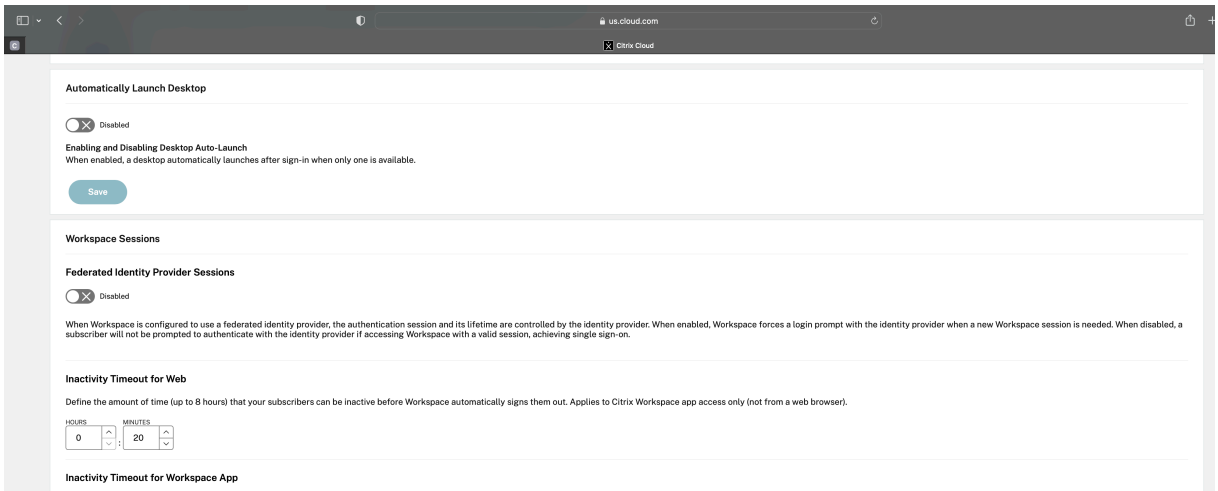
Habilitar la autenticación con Okta para espacios de trabajo

Para obtener más información sobre cómo habilitar la autenticación con Okta, consulte Habilitar la autenticación de Okta para espacios de trabajo.

Configurar la derivación de la autenticación de varios factores (MFA) de Okta

Crear una zona de red que defina un conjunto de direcciones IP que deben incluirse en la lista de permitidos para acceder a la configuración. Para obtener más información, consulte Crear zonas para direcciones IP.

Asegúrese de inhabilitar la opción **Sesiones de proveedores de identidad federada**. Vaya a la consola en la nube, en **Configuración de Workspace** > **Personalizar** > **Preferencias**, y desactive las **Sesiones de proveedores de identidad federada**.



Configurar el agente IWA de Okta

El agente de IWA para Okta es un agente web ligero de Internet Information Services (IIS) que permite el Single Sign-on de escritorio (DSSO) en el servicio Okta.

El DSSO se usa si un equipo unido a un dominio accede a Citrix Cloud. Este equipo unido a un dominio no requiere que se le solicite la autenticación.

1. Asegúrese de que se cumple la siguiente lista de requisitos previos.

   Para obtener la lista de requisitos previos para instalar el agente web de IWA para Okta, consulte Requisitos previos de instalación del agente web de IWA para Okta.

2. Instalar el agente IWA para Okta.

   Para instalar el agente web de IWA para Okta, consulte Instalar el agente web de IWA para Okta..

3. Configurar un explorador de Windows para el SSO.

   Para configurar el explorador de Windows para el SSO, consulte Configurar exploradores de Windows para el SSO.

4. Pruebe el agente web de IWA para Okta.

   Tras descargar e instalar el agente web de IWA para Okta, verifique que el servidor de IWA funciona desde una máquina cliente.

   Si el agente de Okta está configurado correctamente, aparecen los detalles relacionados con **UserPrincipalName** y **SecurityIdentifier**.

   Para obtener más información sobre cómo verificar, consulte Probar el agente web de IWA para Okta.

Configurar la regla de redirección de IdP

Para configurar la regla de **redirección del proveedor de identidades**, consulte Configurar la regla de redirección del proveedor de identidades.

> **Nota:**
>
> En el campo **IdP(s)**, asegúrese de seleccionar **OnPremDSSO**.

Configurar IdP Okta con la consola de administración de Google

1. Para crear una aplicación de lenguaje de marcado de aserción de seguridad (SAML), consulte Crear integraciones de aplicaciones SAML.

   Asegúrese de introducir una URL en los campos **URL de Single Sign-On** y **URI de audiencia (ID de entidad SP)**. Por ejemplo, `https://admin.google.com`.

> **Nota:**
>
> Es posible que tengas que modificar la URL de ejemplo después de crear el perfil SAML en la consola de administración de Google. Consultar los pasos siguientes para obtener más información.

2. Configurar SAML con un proveedor de identidades de terceros en la consola de administración de Google.

   Para crear un perfil de SSO para su organización y asignar los usuarios, siga los pasos que se indican en el enlace Crear un perfil para SSO con SAML.

   Para obtener la información de inicio, cierre de sesión, emisor y otra información de proveedor de identidades de Okta para el perfil de SAML, sigue los pasos que se indican en el enlace Agregar un proveedor de identidades SAML.

3. Para configurar un perfil SAML, consulte el enlace Cómo configurar SAML 2.0 para Google Workspace.

4. Configurar un perfil SAML en OKTA con los detalles del perfil SAML de Google para sincronizar los perfiles:

   a) Vaya a **Seguridad** > **Autenticación** > **SSO con un IdP de terceros** > **Perfiles de SSO de terceros** > abra su perfil de SAML.

   b) En la página del panel de control de Okta (IdP), agregar los detalles del perfil SAML de (proveedor de servicios) Google.

      - Vaya a **URL de Single Sign-On > URL de ACS** y seleccione la opción **Usar esto para URL de destinatario** y **URL de destino**.
      - Vaya a **URI de audiencia (ID de entidad de proveedor de servicios)** > **ID de entidad**.

      Una vez sincronizados los perfiles SAML del IdP y del SP (proveedor de servicios), la página de inicio de sesión de los usuarios gestionados aparece en la página de inicio de sesión de Okta del Chromebook.

5. Asigne usuarios a su aplicación SAML de OKTA.

   Para obtener más información sobre cómo asignar usuarios, consulta el enlace Asignar una integración de aplicaciones a un usuario.

Puntos de control de validación

- Cuando los usuarios agregan la cuenta empresarial de Google en el Chromebook, pueden iniciar sesión con las credenciales de Okta.

- Tras iniciar sesión en el Chromebook, el usuario debe poder abrir el explorador Google Chrome e introducir la URL de Citrix Workspace.
- El usuario debe poder ver la interfaz de usuario de la aplicación Citrix Workspace. El usuario debe poder ir a las aplicaciones y escritorios virtuales sin que se le soliciten las credenciales.

> **Nota:**
>
> Si el SSO no funciona, revise el paso Configurar el proveedor de identidades Okta con la consola de administración de Google.

Configurar el SSO para la aplicación Citrix Workspace para ChromeOS con la extensión de Chrome SAML SSO

Para configurar el SSO mediante la extensión SAML, haga lo siguiente:

1. Instale y configure la extensión SAML SSO para la aplicación Chrome en los dispositivos Chrome.

   Para instalar la extensión, haga clic en SAML SSO for Chrome Apps.
2. La extensión obtiene cookies de SAML del explorador web y las suministra la aplicación Citrix Workspace para ChromeOS.
3. Configure la extensión con la siguiente directiva para permitir que Citrix Workspace obtenga las cookies de SAML. Sustituya el dominio por el dominio IdP de Okta.

```
{

    "whitelist" : {

        "Value" : [
            {

                "appId" : "haiffjcadagjlijoggckpgfnoeiflnem",
                "domain" : "<domain.okta.com>"
                 }

            ]
         }

 }

<!--NeedCopy-->
```

> **Nota:**
>
> Si va a reempaquetar la aplicación Citrix Workspace para ChromeOS, sustituya `haiffjcadagjlijoggckpgfnoeiflnem` por el appID reempaquetado.

4. Implemente FAS para realizar el Single Sign-On en Virtual Apps and Desktops.

   Para realizar el inicio de sesión único en Virtual Apps and Desktops, puede implementar un servicio de autenticación federada (FAS) o configurar la aplicación Citrix Workspace.

   > **Nota:**
   >
   > - Sin FAS, se le pedirán el nombre de usuario y la contraseña de Active Directory. Para obtener más información, consulte Habilitar Single Sign-On para espacios de trabajo con el Servicio de autenticación federada de Citrix.

Single Sign-on en la aplicación Citrix Workspace con Microsoft Azure como proveedor de identidades

May 16, 2024

Puede configurar el inicio de sesión único (SSO) de SAML (Security Assertion Markup Language) para dispositivos ChromeOS. Use Microsoft Entra ID (antes conocido como Azure Active Directory) como proveedor de identidades de SAML y Google Admin como proveedor de servicios (SP).

Puede configurar esta función solo para usuarios gestionados. Como caso de uso, hemos agregado máquinas virtuales de Citrix al Active Directory (AD) local que se crea en Azure. Si tiene máquinas virtuales basadas en AD locales en Azure y usuarios con Microsoft Entra ID, consulte este artículo.

Requisitos previos

Los siguientes requisitos previos requieren privilegios de administrador:

- Active Directory (AD)

  Instale y configure un controlador de dominio activo en su configuración. Para obtener más información, consulte Instalación de AD DS mediante el Administrador del servidor. Para instalar Active Directory Domain Services mediante el Administrador del servidor, siga los pasos del 1 al 19.

- Entidad de certificación (CA)

  Instale CA. Para obtener más información, consulte Instalar la entidad emisora de certificados.

  Una entidad de certificación se puede instalar y configurar en cualquiera de las siguientes máquinas:

  - una nueva máquina dedicada

  - una máquina de CA existente
  - una instalación de este componente de entidad de certificación en Citrix Cloud Connector
  - la máquina de Active Directory

- Citrix Cloud y Citrix Cloud Connector

  Si es la primera vez que usa Citrix Cloud, defina una ubicación de recursos y configure los conectores. Se recomienda tener al menos dos Cloud Connector implementados en entornos de producción. Para obtener información sobre la instalación de Citrix Cloud Connector, consulte Instalación de Cloud Connector.

- Cuenta de administrador global en Azure Portal

  Debe ser un administrador global en Microsoft Entra ID. Este privilegio le ayuda a configurar Citrix Cloud para usar el Entra ID como proveedor de identidades. Para obtener información sobre los permisos que Citrix Cloud solicita al conectarse y usar Entra ID, consulte Permisos de Azure Active Directory para Citrix Cloud.

- Servicio de autenticación federada (opcional).

  Para obtener más información, consulte Habilitar Single Sign-On para espacios de trabajo con el Servicio de autenticación federada de Citrix.

- Cuenta de administrador global en la consola de administración de Google
- Aplicación Citrix Workspace

Introducción

Para empezar, haga lo siguiente:

- Una todas las máquinas al dominio antes de configurar el software o los roles instalados en ellas.
- Instale el software Citrix Cloud Connector en la máquina correspondiente, pero no configure nada todavía.
- Instale Citrix FAS en la máquina correspondiente, pero no configure nada todavía.

Cómo configurar Citrix Cloud para usar Azure AD como proveedor de identidades

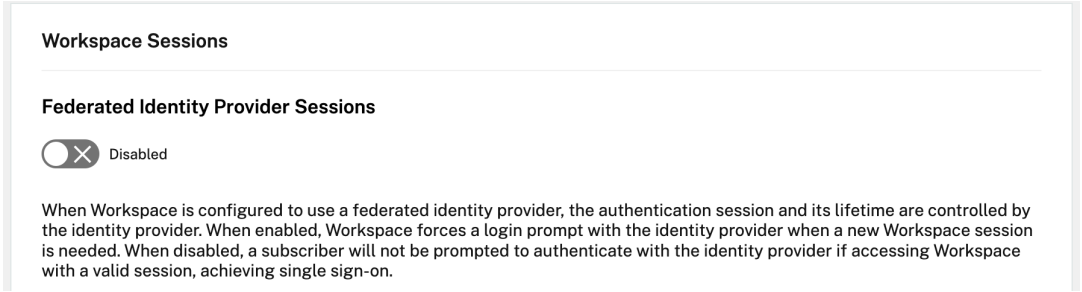
> **Nota:**
>
> Asegúrese de cumplir todos los requisitos previos.

1. Para conectar Entra ID a Citrix Cloud, consulte Conectar Azure Active Directory a Citrix Cloud.

2. Para agregar administradores a Citrix Cloud desde Entra ID, consulte Agregar administradores a Citrix Cloud desde Azure AD.
3. Para iniciar sesión en Citrix Cloud con Entra ID, consulte Iniciar sesión en Citrix Cloud con Azure AD.
4. Para habilitar las capacidades avanzadas de Entra ID, consulte Habilitar las funciones avanzadas de Azure AD.
5. Para volver a conectarse a Entra ID para la aplicación actualizada, consulte Reconectarse a Azure AD para la aplicación actualizada.
6. Para volver a conectar Entra ID, consulte Reconectarse a Azure AD para la aplicación actualizada.
7. Para sincronizar cuentas con Entra ID Connect, consulte Sincronizar cuentas.

   Se recomienda sincronizar las cuentas de AD locales con el Entra ID.

   > **Nota:**
   >
   > Inhabilite la solicitud de inicio de sesión para las sesiones de proveedores de identidades federados en la configuración de Citrix Workspace.



Configurar el SSO y el aprovisionamiento de usuarios entre Microsoft Azure y ChromeOS en el portal de Azure

Tras configurar el aprovisionamiento del SSO entre un arrendatario de Microsoft Entra ID y Google para ChromeOS, los usuarios finales pueden iniciar sesión en una página de autenticación de Azure en lugar de hacerlo en la pantalla de inicio de sesión de Google de sus dispositivos con ChromeOS.

Para obtener más información, consulte:

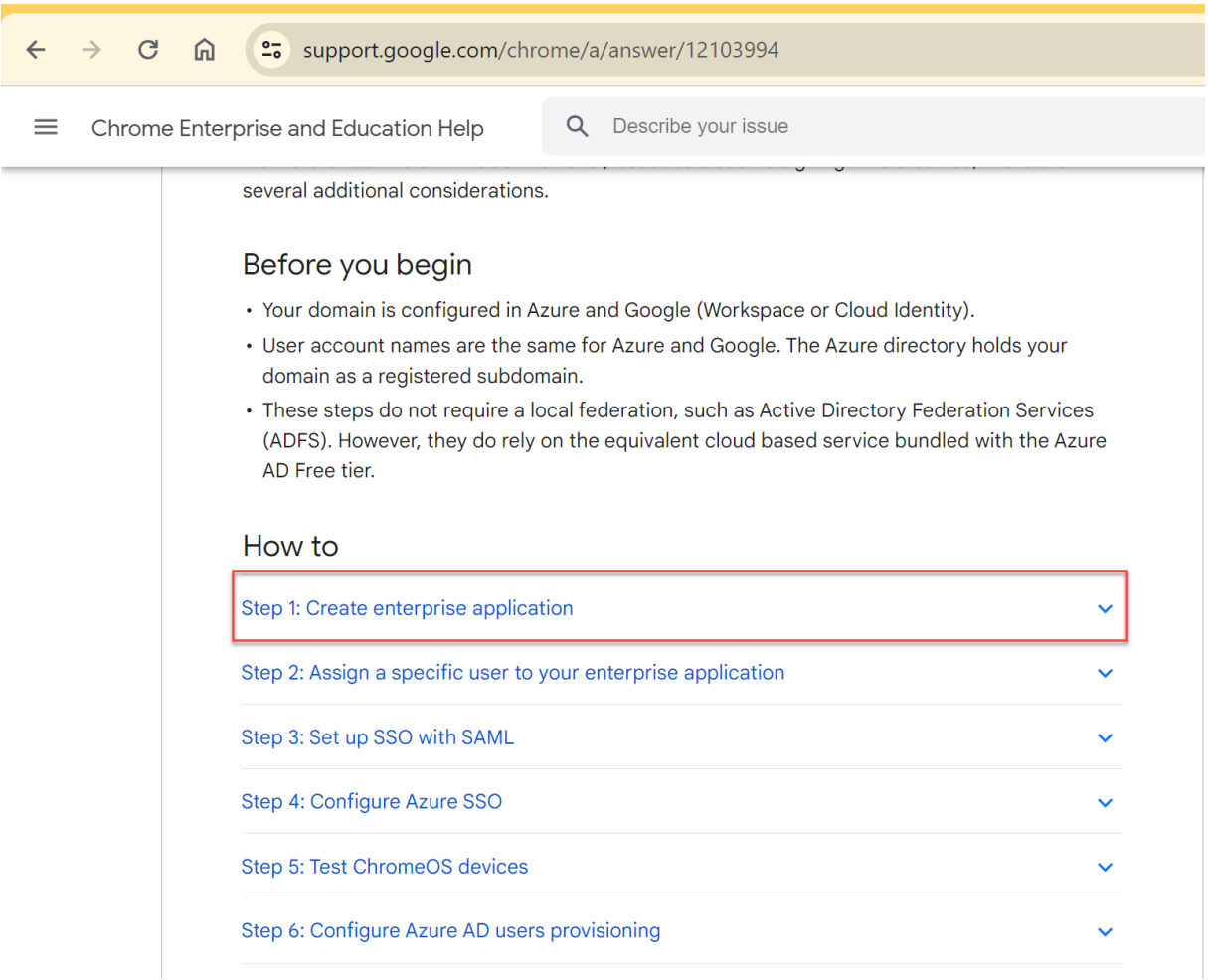
- El artículo de Google Configurar el SSO y aprovisionamiento de usuarios entre Microsoft Azure y ChromeOS.

y

- El tutorial Microsoft Entra ID SSO integration with Google Cloud / G Suite Connector by Microsoft.

Para configurar el SSO en el portal de Azure:

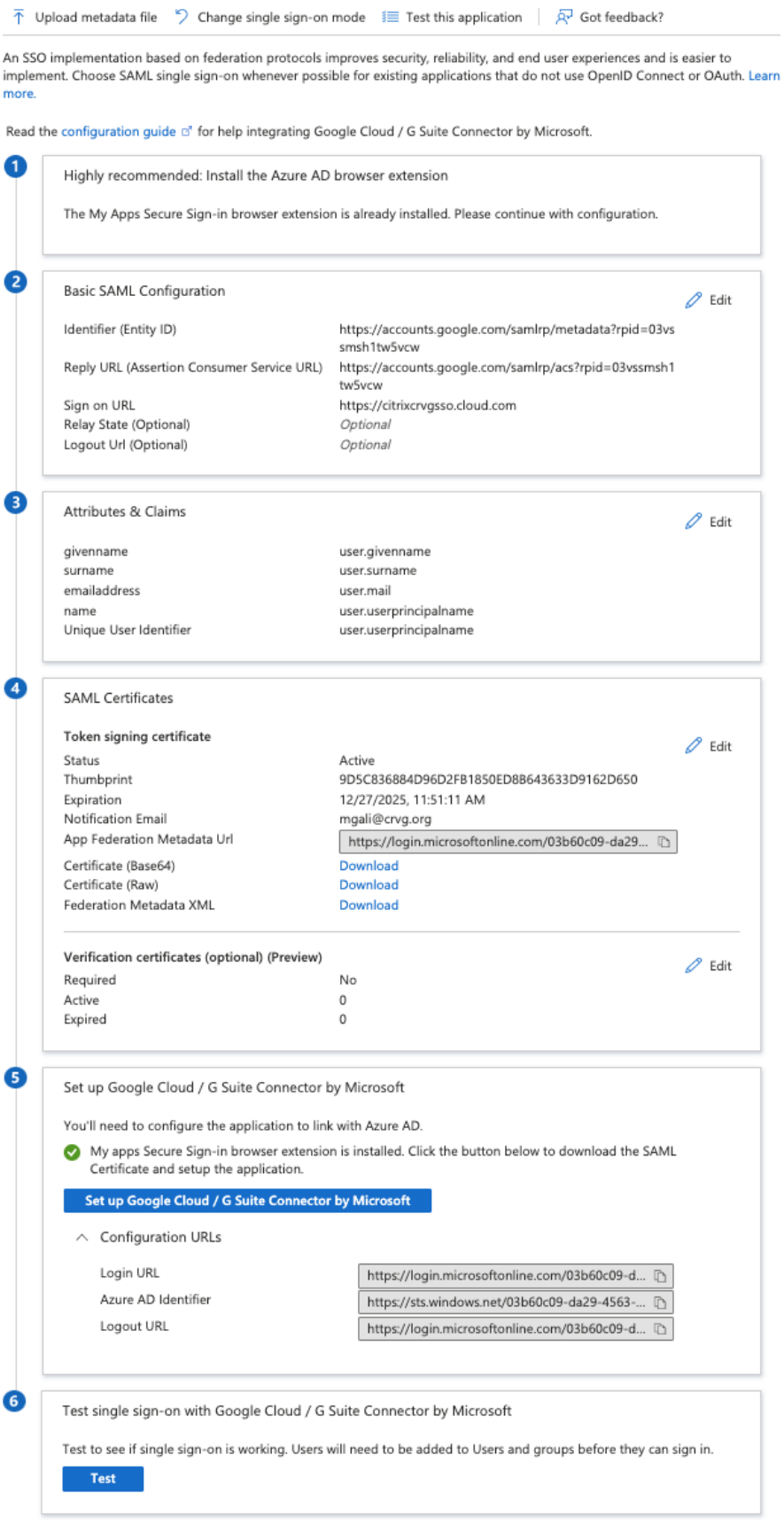
1. Cree una aplicación empresarial en el portal de Microsoft Entra ID. Para obtener más información, consulte el paso 1 del artículo de Google Configurar el SSO y el aprovisionamiento de usuarios entre Microsoft Azure y ChromeOS.



1. Asigne uno o varios usuarios a la aplicación empresarial que creó en el paso 1. Para obtener más información, consulte el paso 2 del artículo de Google Configurar el SSO y el aprovisionamiento de usuarios entre Microsoft Azure y ChromeOS.
2. Configure SSO con SAML. Para obtener más información, consulte el paso 3 del artículo de Google Configurar el SSO y el aprovisionamiento de usuarios entre Microsoft Azure y ChromeOS.

   > **Nota:**
   >
   > Se recomienda cambiar la configuración básica de SAML después de crear la directiva de SAML en la directiva administrativa de Google.

   Después de configurar las URL en el portal de Azure para el inicio de sesión único basado en SAML, la aplicación se muestra de la siguiente manera.



> **Punto de control de validación**
>
> Al introducir la URL del almacén, debe mostrarse la página de inicio de sesión del proveedor de identidades de Azure. Si no funciona, vuelva a consultar los pasos de Configurar el SSO y el aprovisionamiento de usuarios entre Microsoft Azure y ChromeOS en el portal de Azure.

Configure el perfil de SSO de SAML con la consola de administración de Google

- Agregue el dominio y los usuarios y cree una OU. Para obtener más información, consulte la Guía completa de las unidades organizativas de Google.
- Cree el perfil de SAML SSO con el Microsoft Entra ID como proveedor de identidades. Para obtener más información, consulte Configuración del inicio de sesión único (SSO) de SAML para usuarios de Azure AD.

> **Punto de control de validación**
>
> Debe poder iniciar sesión con Chromebook en la aplicación Citrix Workspace usando las credenciales de Azure. Al introducir la URL del almacén en el explorador web, debe poder iniciar sesión.

Configurar el SSO para la aplicación Citrix Workspace para ChromeOS con la extensión de Chrome SAML SSO

Para configurar el SSO mediante la extensión SAML, haga lo siguiente:

1. Instale y configure la extensión SAML SSO para la aplicación Chrome en los dispositivos Chrome.

   Para instalar la extensión, haga clic en SAML SSO for Chrome Apps.

2. La extensión obtiene cookies de SAML del explorador web y las suministra la aplicación Citrix Workspace para ChromeOS.

3. Configure la extensión con la siguiente directiva para permitir que la aplicación Citrix Workspace obtenga las cookies de SAML. A continuación se muestran los datos de JSON:

```
{

"allowlist": {

    "Value": [
        {

            "appId": "haiffjcadagjlijoggckpgfnoeiflnem",
            "domain": "login.microsoftonline.com"
         }

    ]
```



```
13   }
14
15   }
16
17 <!--NeedCopy-->
```

> **Punto de control de validación**
>
> Al iniciar la aplicación Citrix Workspace con la extensión SSO y el almacén del proveedor de identidades de Azure, el inicio de sesión en la aplicación Citrix Workspace debe realizarse correctamente.

Implemente FAS para efectuar el inicio de sesión único en Virtual Apps and Desktops

Para lograr el SSO para aplicaciones y escritorios virtuales, puede implementar un Servicio de autenticación federada (FAS).

> **Nota:**
>
> Sin FAS, se le pedirán el nombre de usuario y la contraseña de Active Directory. Para obtener más información, consulte Habilitar Single Sign-On para espacios de trabajo con el Servicio de autenticación federada de Citrix.

SDK y API

May 16, 2024

HDX SDK

La aplicación Citrix Workspace para ChromeOS presenta una API (Experimental API) que permite a aplicaciones Chrome de terceros bloquear, desbloquear y desconectarse de:

- Citrix Virtual Apps and Desktops
- Sesiones de Citrix DaaS (antes denominado Citrix Virtual Apps and Desktops Service)

Con esta API, puede iniciar la aplicación Citrix Workspace para ChromeOS tanto en modo integrado como en modo quiosco. Las sesiones iniciadas en el modo incrustado funcionan de manera similar a las sesiones iniciadas en el modo quiosco.

Para ver la documentación del SDK, consulte HDX SDK for Citrix Workspace app for ChromeOS.

Para ver ejemplos de HDX SDK, consulte la página de descargas de Citrix.

Citrix Virtual Channel SDK

El Citrix Virtual Channel Software Development Kit (SDK) le permite escribir aplicaciones del lado del servidor y controladores del lado del cliente para canales virtuales adicionales que usan el protocolo ICA.

Las aplicaciones de canal virtual del lado del servidor se encuentran en servidores Citrix Virtual Apps o Citrix Virtual Apps and Desktops. Esta versión del SDK le permite escribir nuevos canales virtuales para la aplicación Citrix Workspace para ChromeOS. Si quiere escribir controladores virtuales para otras plataformas cliente, contacte con Citrix.

El Virtual Channel SDK ofrece:

- Una sencilla interfaz que se puede usar con los canales virtuales en el Citrix Server API SDK (WFAPI SDK) para crear nuevos canales virtuales.
- Código fuente operacional de varios ejemplos de programas de canales virtuales, que demuestran varias técnicas de programación.
- El Virtual Channel SDK requiere el SDK de WFAPI para escribir la parte del lado del servidor del canal virtual.

Para ver la documentación del VC SDK, consulte Citrix Virtual Channel SDK for Citrix Workspace app for ChromeOS.

Mejoras en Virtual Channel SDK

A partir de la versión 2305, la aplicación Citrix Workspace para ChromeOS admite las API de administración de ventanas en el Virtual Channel SDK. Las API web permiten a los administradores de TI crear aplicaciones interactivas y personalizarlas para sus usuarios finales.

Procedimiento para consumir la API en la aplicación Chrome de terceros

1. Instale la versión más reciente de la aplicación Citrix Workspace para ChromeOS. Consulte la página Descargas de Citrix para ver más información.
2. Para agregar la aplicación Chrome de terceros a la lista de permitidos, agregue el archivo de directiva de la aplicación Citrix Workspace para ChromeOS. Use los parámetros de administración de Chrome para agregar la directiva.

   Para obtener más información, consulte Administración de aplicaciones Chrome por unidad organizativa en Google Support.

   Para agregar la aplicación Chrome de terceros a la lista de permitidos, estos son los datos JSON del `policy.txt` de muestra:


```
{

      "settings": {

              "Value": {

              "settings_version": "1.0",
              "store_settings": {

              "externalApps": [“ <3rdParty_App1_ExtnID>” ,“ <3rdParty_App2_ExtnID>” ]
                                    }

                          }

                  }

 }

<!--NeedCopy-->
```

> **Nota:**
>
> <3rdParty_App1_ExtnID> se usa como ejemplo para el nombre de externalApps y puede enviar mensajes a la aplicación Citrix Workspace para ChromeOS. Obtenga el **appid** desde el sitio chrome://extensions.

3. Inicie la sesión de escritorio o de aplicación en Citrix Workspace para ChromeOS de esta manera:

- Obtenga el workspaceappID

```
var workspaceappID = "haiffjcadagjlijoggckpgfnoeiflnem ";
```

> **Nota:**
>
> En este ejemplo, **workspaceappID** indica la versión de la tienda de aplicaciones de la aplicación Citrix Workspace para ChromeOS. Si usa una versión reempaquetada de la aplicación Citrix Workspace para ChromeOS, use el workspaceappID apropiado.

- Convierta los datos ICA desde INI al formato JSON.

> **Nota:**
>
> Normalmente, el archivo ICA se obtiene desde StoreFront como un archivo INI. Use esta función auxiliar para convertir un archivo ICA de INI a JSON.

```
//Helper function to convert ica in INI format to JSON
function convertICA_INI_TO_JSON(data){

var keyVals = {
```



```
 }
;
if (data) {

var dataArr;
if(data.indexOf('\r')===-1){

dataArr = data.split('\n');
 }
else{

dataArr = data.split('\r\n');
 }

for (var i = 0; i < dataArr.length; i++) {

var nameValue = dataArr[i].split('=', 2);
if (nameValue.length === 2) {

keyVals[nameValue[0]] = nameValue[1];
 }

// This is required as LaunchReference contains '=' as well. The above split('=',2) will not provide
// the complete LaunchReference. Ideally, something like the following should be used generically as well
// because there can be other variables that use the '=' character as part of the value.
if (nameValue[0] === "LaunchReference") {

var index = dataArr[i].indexOf('=');
var value = dataArr[i].substr(index + 1);
keyVals[nameValue[0]] = value;
 }

 }

console.log(keyVals);//to remove
return keyVals;
 }

return null;
 }


<!--NeedCopy-->
```

- Envíe un mensaje ICA desde la aplicación Chrome de terceros a la aplicación Citrix Workspace para ChromeOS.

```
var icaFileJson = {
... }
; // ICA file passed as JSON key value pairs.
```



```
var message = {

"method" : "launchSession",
"icaData" : icaJSON
 }
;
chrome.runtime.sendMessage(workspaceappID, message,
function(launchStatus) {

if (launchStatus.success) {

// handle success.
console.log("Session launch was attempted successfully");
 }
 else {

// handle errors.
console.log("error during session launch: ", launchStatus.message
    );
 }

 }
);

<!--NeedCopy-->
```

Para obtener más detalles sobre los comandos **sendMessage** de la API, consulte estos enlaces:

https://developer.chrome.com/extensions/runtime#event-onMessageExternal

https://developer.chrome.com/extensions/runtime#method-sendMessage

Compatibilidad con Manifest V3 en supuestos de SDK

A partir de la versión 2305, la aplicación Citrix Workspace para ChromeOS admite que HDX SDK con extensiones de Chrome tenga Manifest versión 3.

Para obtener más información, consulte Citrix Workspace app for ChromeOS HDX SDK en la documentación para desarrolladores.

Elementos retirados

May 16, 2024

Los anuncios de este artículo le avisan con antelación de las plataformas, los productos Citrix y las funciones que se están retirando progresivamente. Con estos anuncios, puede tomar decisiones comerciales oportunas.

Citrix analiza el uso que hacen los clientes de una función que está por retirar y los comentarios que tengan sobre la eliminación de la función para determinar cuándo retirarla. Estos anuncios están sujetos a cambios en las versiones posteriores y es posible que no contengan todas las funciones o funciones retiradas.

Los elementos obsoletos no se eliminan inmediatamente. Citrix sigue admitiéndolos en la presente versión, pero en el futuro se quitarán.

Elemento	Retirada anunciada en	Eliminado en	Alternativa
Ninguna por ahora	-	-	-