



Aplicación Citrix Workspace para Mac

Contents

Acerca de esta versión	3
Requisitos del sistema y compatibilidad	24
Instalación, desinstalación y actualización	30
Update	32
Configuración	39
Autenticarse	77
Proteger comunicaciones	79

Acerca de esta versión

February 21, 2022

Importante

A partir de macOS Catalina, Apple ha impuesto requisitos adicionales para los certificados de CA raíz y los certificados intermedios que los administradores deben configurar. Para obtener más información, consulte el artículo [HT210176](#) de la página de soporte de Apple.

Novedades en la versión 2201

Migración de StoreFront a Workspace [Tech Preview]

A medida que su organización migra de una instancia local de StoreFront a Workspace, los usuarios deben agregar manualmente la nueva URL de Workspace en la aplicación Workspace. Esta función permite a los administradores migrar fácilmente a los usuarios de un almacén de StoreFront a un almacén de Workspace con una interacción mínima de los usuarios.

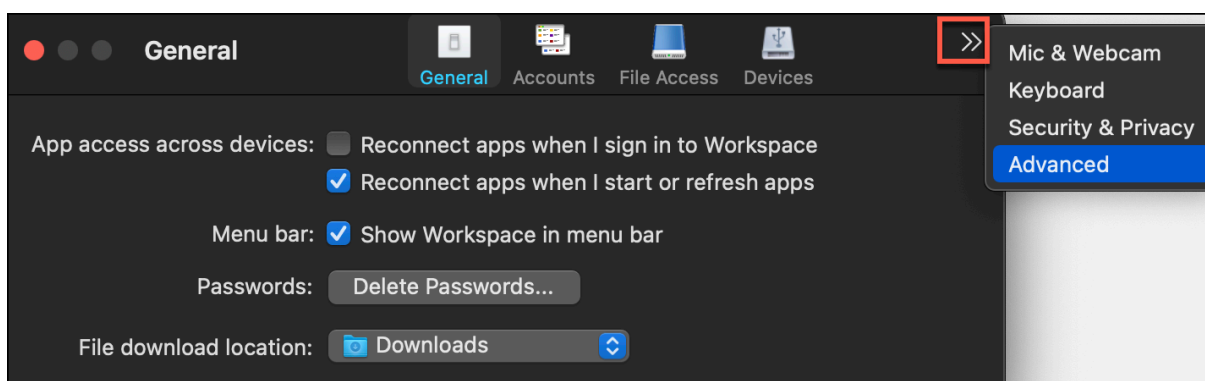
Nota:

Las Technical Previews están disponibles para que los clientes las prueben en sus entornos de producción limitados o en entornos que no son de producción y compartan sus comentarios. Citrix no acepta casos de asistencia para funciones en Tech Preview, pero agradece [comentarios](#) para mejorarlas. Citrix puede o no actuar a partir de los comentarios en función de su gravedad e importancia. No es aconsejable implementar compilaciones beta en entornos de producción.

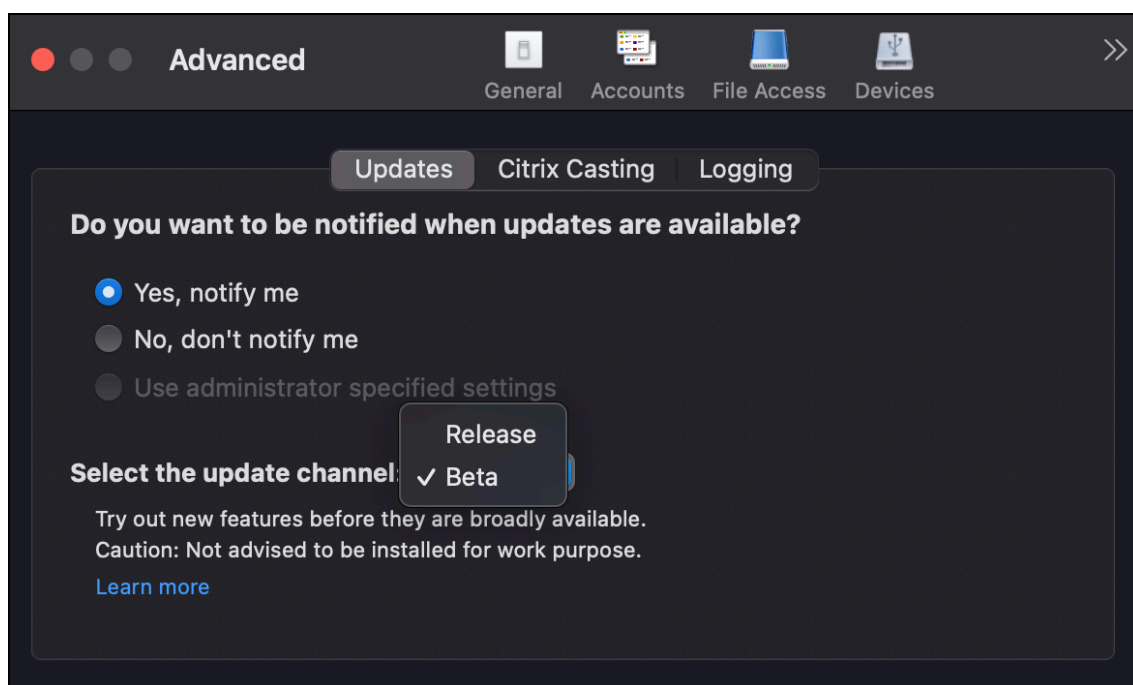
Programa Beta de la aplicación Citrix Workspace

A partir de esta versión, podrá actualizar automáticamente las instalaciones existentes de Citrix Workspace a las compilaciones Beta más recientes y probarlas. Las compilaciones Beta son versiones de acceso anticipado publicadas antes de la disponibilidad general de actualizaciones públicas, estables y totalmente funcionales. Recibirá una notificación de actualización cuando la Citrix Workspace se haya configurado para obtener actualizaciones automáticas.

Para acceder a las compilaciones Beta, abra la aplicación Workspace, haga clic con el botón secundario en Citrix Workspace, en la barra de herramientas, y haga clic en **Preferencias > Avanzado**. Para actualizar su versión a una compilación Beta, seleccione el **canal Beta** de la lista desplegable.



- **Beta:** Versión de acceso anticipado para probar y notificar problemas fácilmente antes de su disponibilidad general.
- **Público:** Actualización pública, estable y totalmente funcional.



Para obtener más información sobre el uso de esta función, consulte [Actualización](#).

Prolongar varios monitores en el modo de pantalla completa [Tech Preview]

Ahora puede acceder al modo de pantalla completa en dos o más monitores simultáneamente. Para usar esta función, siga estos pasos:

1. Abra Citrix Viewer.
2. Para usar el modo de pantalla completa en los demás monitores conectados, arrastre la ventana desde el monitor principal hasta abarcar los monitores conectados. En la barra de herramientas

de Citrix Viewer, seleccione **Entrar en pantalla completa**. La ventana pasa al modo de pantalla completa en esos monitores.

Nota:

Si seleccionó la opción **Usar todas las pantallas en pantalla completa**, anule la selección porque esta selección prolonga la pantalla completa en todos los monitores conectados.

3. Arrastre la ventana de Citrix Virtual Desktop a un monitor para entrar en el modo de pantalla completa.

Citrix recomienda usar 3 monitores como máximo, incluido el monitor principal.

Nota:

Las Technical Previews están disponibles para que los clientes las prueben en sus entornos de producción limitados o en entornos que no son de producción y compartan sus comentarios. Citrix no acepta casos de asistencia para funciones en Tech Preview, pero agradece [comentarios](#) para mejorarlas. Citrix puede o no actuar a partir de los comentarios en función de su gravedad e importancia. No es aconsejable implementar compilaciones beta en entornos de producción.

Problemas resueltos en la versión 2201

- Al seleccionar el texto candidato en la ventana de redacción del Editor de métodos de entrada (IME) con las flechas izquierda o derecha del teclado, el cursor de entrada de texto no se mueve como es debido. Este problema se produce al iniciar un escritorio con la casilla **Utilizar la distribución local del teclado en vez de la distribución de teclado del servidor remoto** seleccionada en la ventana **Preferencias > Teclado** de la aplicación Citrix Workspace. Este problema se observa solo en chino y japonés. [HDX-34956]
- El puntero del mouse desaparece de forma intermitente en sesiones de aplicaciones de Workspace y no puede hacer clic en nada. [HDX-36820]
- La sesión de escritorio se cierra de forma inesperada al arrastrar una celda de una tabla dinámica en una hoja de Excel. [HDX-37178]
- A veces, hay problemas con los gráficos de la sesión de escritorio después de actualizarse a la versión 2112 y cuando se aplican directivas de códec H.264 sin pérdida y de pantalla completa. [HDX-37272]
- Después de actualizar la versión 2010 de la aplicación Workspace a la versión 2112, no puede conectarse a escritorios ni a aplicaciones. [RFMAC-10811]

Problemas conocidos en la versión 2201

- El nombre del cliente contiene caracteres aleatorios en Citrix Broker Service y Citrix Director si utiliza la aplicación Workspace en el modo sin conexión (intranet). [RFMAC-10842]

Versiones anteriores

En esta sección se enumeran las funciones de versiones anteriores junto con sus problemas resueltos y conocidos. Las versiones llegan al fin de su vida (EOL) 18 meses después de publicarse. Para obtener información detallada sobre las fechas del ciclo de vida de las versiones compatibles, consulte [Lifecycle Milestones for Citrix Workspace app and Citrix Receiver](#).

2112

Novedades

Compatibilidad con almacenes web personalizados

Ahora puede acceder al almacén web personalizado de su organización desde la aplicación Citrix Workspace para Mac. Antes, accedía a todos los almacenes personalizados solamente a través del explorador.

La aplicación Citrix Workspace para Mac carga los almacenes web personalizados con una experiencia similar a la de un explorador web y amplía las prestaciones de protección de aplicaciones a los almacenes web personalizados. Al hacer que el portal personalizado sea accesible desde la aplicación Workspace nativa, se ofrecen prestaciones y una experiencia de usuario integrales para esta función. Para obtener más información detallada sobre Global App Configuration Service, consulte [Getting Started](#).

Para obtener más información sobre la configuración de almacenes web personalizados, consulte [Almacenes web personalizados](#).

Solicitar control en Microsoft Teams

En esta versión, durante una llamada de Microsoft Teams, puede solicitar el control cuando un participante comparte la pantalla. Una vez que tenga el control, puede realizar selecciones, modificaciones u otras acciones en la pantalla compartida.

Para tomar el control cuando se comparte una pantalla, haga clic en **Solicitar control** en la parte superior de la pantalla de Microsoft Teams. El participante de la reunión que comparte la pantalla puede aceptar o rechazar su solicitud. Cuando haya terminado, haga clic en **Liberar control**.

Limitación:

La opción **Solicitar el control** no está disponible durante llamadas entre un usuario optimizado y un usuario en el cliente de escritorio de Microsoft Teams nativo en el dispositivo de punto final. Como solución temporal, los usuarios pueden unirse a una reunión para obtener la opción **Solicitar el control**.

e911 dinámico

Con esta versión, la aplicación Citrix Workspace admite llamadas de emergencia dinámicas. Cuando se usa en los planes de llamadas de Microsoft, Operator Connect y enrutamiento directo, le permite:

- Configurar y redirigir llamadas de emergencia.
- Notificar al personal de seguridad.

La notificación se proporciona en función de la ubicación actual de la aplicación Workspace que se ejecuta en el dispositivo de punto final, en lugar del cliente de Microsoft Teams que se ejecuta en el 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 2112.1 para Windows, la optimización para Microsoft Teams con HDX cumple con la ley de Ray Baum. Para obtener más información sobre esta función, consulte [Compatibilidad con e911 dinámico](#) en la sección **Sistema telefónico de Microsoft**.

Impresión universal de PDF (Technical Preview)

La función de impresión universal de PDF está disponible en la versión 2112 de Citrix Virtual Apps and Desktops. Esta función está inhabilitada de forma predeterminada. Para usarla, debe registrarse mediante [este formulario web](#). La función se activa para usted una vez recibida su información. También obtendrá instrucciones sobre el uso de la función y las directivas de impresión que deben habilitarse.

Nota:

Las Technical Previews están disponibles para que los clientes las prueben en sus entornos de producción limitados o en entornos que no son de producción y compartan sus comentarios. Citrix no acepta casos de asistencia para funciones en Tech Preview, pero agradece comentarios para mejorarlas. Citrix puede o no actuar a partir de los comentarios en función de su gravedad e importancia. No es aconsejable implementar compilaciones beta en entornos de producción.

Continuidad del servicio

La continuidad del servicio elimina o minimiza la dependencia de la disponibilidad de los componentes involucrados en el proceso de conexión. Los usuarios pueden iniciar sus aplicaciones y escritorios virtuales, independientemente del estado de los servicios en la nube. Las extensiones web de Citrix Workspace ponen la continuidad del servicio a disposición de los usuarios que acceden a sus aplicaciones y escritorios a través de un explorador.

Juntos, la aplicación Workspace y la extensión web de Workspace utilizan las concesiones de conexión de Workspace para proporcionar a los usuarios del explorador acceso a sus aplicaciones y escritorios durante las interrupciones. Para obtener más información, consulte [Continuidad del servicio](#).

Citrix Workspace Browser

Esta versión de Workspace Browser está basada en Chromium 95. Para ver las funciones y correcciones de errores de Citrix Workspace Browser, consulte [Novedades](#) en la documentación de Citrix Workspace Browser.

Problemas resueltos

- El error “No se puede conectar con el servidor” aparece cuando el protocolo de transporte cambia de Enlightened Data Transport (EDT) a TCP. [CVADHELP-18310]
- Si se abre una aplicación web progresiva (PWA) protegida en macOS, no se aplican las directivas de **protección de aplicaciones**. [RFMAC-10128]

2111

Novedades

- Con esta versión, los usuarios no pueden revertir manualmente la aplicación Citrix Workspace para Mac a una versión anterior a la versión instalada en sus sistemas. Por ejemplo, si un dispositivo Mac tiene la versión 2109 de la aplicación Citrix Workspace instalada, no podrá revertir manualmente la aplicación a la versión 2108 o a una anterior.
- Inicie la sesión de escritorio remoto con una licencia permanente si usa licencias de acceso de cliente (CAL) para acceder a escritorios remotos. Puede iniciar la sesión de escritorio remoto cuando el ID de cliente tenga más de 15 caracteres.
- Para cargar el SDK de Citrix Virtual Channel en un Mac que use la aplicación Citrix Workspace 2111, debe compilar de nuevo sus canales virtuales personalizados. Para obtener información detallada, consulte [Update Custom Virtual Channels on Citrix Workspace app for Mac](#).

Compatibilidad con almacenes web personalizados [Tech Preview]

Con esta versión, puede acceder al almacén web personalizado de su organización desde la aplicación Citrix Workspace para macOS. Para usar esta función, los administradores deben agregar el almacén web personalizado a la lista de URL permitidas en Global App Configuration Service. Tras agregar las URL, puede proporcionar la URL del almacén web personalizado en la pantalla Agregar cuenta de la aplicación Citrix Workspace. El almacén web personalizado se abre en la aplicación Workspace para macOS nativa.

Nota:

Las Technical Previews están disponibles para que los clientes las prueben en sus entornos de producción limitados o en entornos que no son de producción y compartan sus comentarios. Citrix no acepta casos de asistencia para funciones en Tech Preview, pero agradece [comentarios](#) para mejorarlas. Citrix puede o no actuar a partir de los comentarios en función de su gravedad e importancia. No es aconsejable implementar compilaciones beta en entornos de producción.

Citrix Workspace Browser: Para ver las nuevas funciones y correcciones de errores de Citrix Workspace Browser, consulte [Novedades](#) en la documentación de Citrix Workspace Browser.

Problemas resueltos

- En dispositivos con macOS, no se admite Advanced Audio Coding (AAC). [CTXBR-1844]
- Si configuró la aplicación Workspace mediante el archivo `.cr` e inició sesión con sus credenciales, la página de inicio tarda en aparecer. [RFMAC-9990]
- Abra una aplicación SaaS protegida, abra una ficha nueva y arrastre la ficha nueva fuera de la barra de fichas para separarla en una nueva ventana. Coloque dos ventanas juntas, abra una ficha nueva en la segunda ventana y haga una captura de pantalla. También puede hacer capturas de pantalla de la aplicación SaaS protegida. [RFMAC-10060]
- Si cambia de un almacén a otro, es posible que se le cierre la sesión del primer almacén. [RFMAC-10137]
- Al introducir credenciales incorrectas al iniciar sesión en la aplicación Workspace, no aparece el mensaje de error “Credenciales incorrectas” y aparece de nuevo un mensaje de autenticación. A veces, **Dominio\Usuario** aparece en la solicitud de autenticación en lugar de **Nombre de usuario**. [RFMAC-10210]
- No se pueden realizar llamadas P2P de Microsoft Teams optimizado desde la aplicación Citrix Workspace para Mac 2109 a la aplicación Citrix Workspace para Windows 2109. [HDX-35223]

2109.1

Novedades

Compatibilidad con macOS Monterey

La aplicación Citrix Workspace para Mac se admite en macOS Monterey (12.0.1).

Problemas resueltos

- Si abrió una aplicación protegida, una aplicación SaaS desprotegida y una sesión de escritorio protegida, el explorador web se cierra de forma inesperada. Este problema se produce cuando

cambia de la ventana de la sesión de escritorio protegida a la aplicación SaaS desprotegida. [CTXBR-2087]

- Si el administrador instaló extensiones externas en Google Chrome, Citrix Workspace Browser se cierra de forma inesperada al abrirlo. [CTXBR-2135]

2109

Novedades

Nota:

Si se habilita la Continuidad del servicio y actualiza la versión a 2109, se actualizarán los archivos de concesión de conexiones. Todas las concesiones existentes se eliminan y se obtienen concesiones nuevas como parte de mejoras de funcionalidad.

Aplicación Citrix Workspace para Mac en la Beta de macOS Monterey

La aplicación Citrix Workspace 2109 para Mac se ha probado en la Beta 7 de macOS Monterey. Utilice esta configuración en un entorno de prueba y envíenos sus comentarios.

Precaución:

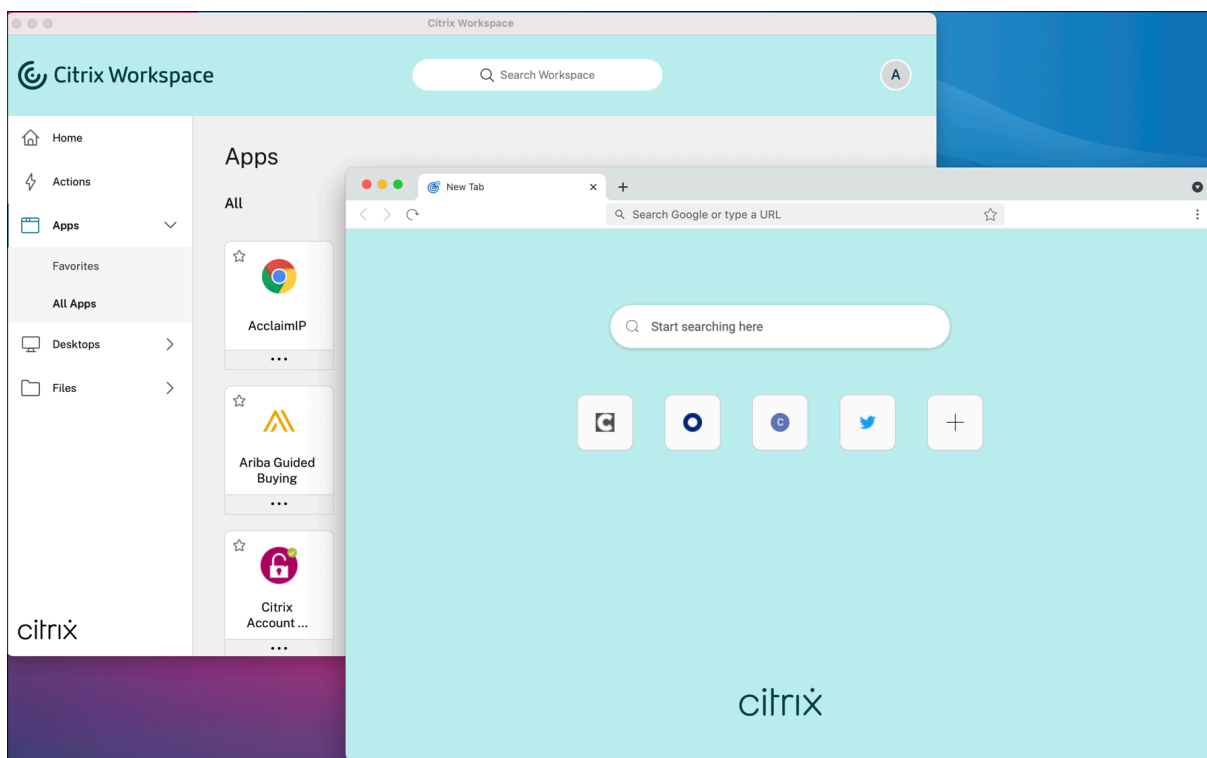
No utilice la aplicación Citrix Workspace para Mac en versiones Beta de macOS Monterey en entornos de producción.

Detección automática de almacenes por dirección de correo electrónico

Ya puede proporcionar su dirección de correo electrónico en la aplicación Citrix Workspace para Mac para detectar automáticamente el almacén asociado a esa dirección de correo electrónico. Si hay varios almacenes asociados a un dominio, de forma predeterminada se agrega el primer almacén devuelto por Global App Configuration Service como el almacén elegido. Los usuarios siempre pueden cambiar a otro almacén si fuera necesario.

Citrix Workspace Browser

Citrix Workspace Browser es un explorador web nativo que se ejecuta en la máquina cliente. Permite a los usuarios abrir aplicaciones web o SaaS desde la aplicación Citrix Workspace de forma segura. El explorador garantiza una interfaz de usuario uniforme al acceder a varias aplicaciones web o SaaS, al tiempo que mejora la productividad y le ofrece un buen rendimiento en la generación de esas aplicaciones.



Con un enfoque continuo en enriquecer la experiencia de usuario, el nuevo explorador de Workspace le ofrece una experiencia mejorada y más nativa con estas funciones:

- Acceso sin VPN a páginas web internas
- Compatibilidad con micrófonos y cámaras web
- Experiencia de navegación por fichas
- Vistas con varias ventanas
- Barra de direcciones (omnibox) modificable
- Marcadores
- Accesos directos en la página de la nueva ficha
- Parámetros personalizables
- Análisis

Los administradores pueden habilitar directivas de protección de aplicaciones o Secure Workspace Access (SWA), como la protección contra el registro de tecleo y las capturas de pantalla, descargas, impresión, restricciones del portapapeles y marca de agua en combinaciones diferentes según la URL.

Para obtener más información, consulte la documentación de [Citrix Workspace Browser](#).

Mejora de End Point Analysis (EPA)

A partir de esta versión, la aplicación Citrix Workspace para macOS admite End Point Analysis (EPA). Advanced Endpoint Analysis (EPA) analiza el dispositivo para buscar requisitos de seguridad de dispositivos de punto final configurados en Citrix Gateway. Cuando el escaneo se completa correctamente,

se concede acceso a los usuarios.

Nota:

Esta función solo está operativa si configuró la autenticación nFactor en su entorno.

Para obtener más información sobre el análisis de EPA, consulte [Advanced Endpoint Analysis scans](#).

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 del entorno y sustituye los formatos de compresión de audio antiguos para proporcionar una excelente experiencia de usuario. Para obtener más información, consulte [Audio adaptable](#).

Compatibilidad de H.264 Advanced Video Coding (MPEG-4 AVC) con Microsoft Teams

Esta versión admite la codificación y la decodificación de vídeo H.264 aceleradas por hardware, lo que reduce la carga en el uso de la CPU y mejora la experiencia de las conferencias de vídeo. Ahora, el motor multimedia de Citrix HDX, que optimiza Microsoft Teams (HdxRtcEngine.exe), utiliza el marco VideoToolbox de Apple para la codificación y la decodificación. Este marco comprime y descomprime vídeo más rápido y en tiempo real. Además, se optimiza la descarga de la codificación y la decodificación a la GPU. La codificación y la decodificación de vídeo aceleradas por hardware están habilitadas de forma predeterminada si los dispositivos las admiten. Esta mejora reduce la carga de la CPU durante el uso multimedia cuando Microsoft Teams está optimizado con HDX.

Problemas resueltos

- Después de iniciar sesión en la aplicación Workspace para Mac, se le solicitará la autenticación unas horas después. [RFMAC-10032]
- Al agregar un almacén en la aplicación Workspace, cambiar el dominio de autenticación en la consola del servidor, dejar la aplicación inactiva durante unos minutos y, a continuación, abrir una sesión de escritorio o aplicación, es posible que la aplicación Workspace se cierre de forma inesperada. [RFMAC-10133]
- Cuando una aplicación o un escritorio virtual ya se están ejecutando y se inicia otra aplicación o escritorio virtual, Citrix Viewer aparece, pero la aplicación virtual no se abre. Este problema ocurre en dispositivos con macOS 11.6. [RFMAC-10134]

2108.1

Novedades

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

Problemas resueltos

Cuando una aplicación o un escritorio virtual ya se están ejecutando y se inicia otra aplicación o escritorio virtual, Citrix Viewer aparece, pero la aplicación virtual no se abre. Este problema ocurre en dispositivos con macOS 11.6. [RFMAC-10134]

2108

Novedades

Ahora Citrix Workspace para Mac permite la detección de unidades de transmisión máxima (MTU) en Enlightened Data Transport (EDT). Aumenta la fiabilidad y la compatibilidad del protocolo EDT y mejora la experiencia de usuario.

Nota:

La detección de MTU en EDT está disponible macOS Big Sur y versiones posteriores.

Problemas resueltos

- Hay un retraso en el vídeo de las llamadas de conferencia en Microsoft Teams. [HDX-32603]
- En clientes Mac con macOS Big Sur, es posible que se produzca un error HTTP 404 o HTTP/1.1 en el servidor interno. El problema se produce al intentar volver a conectarse a las sesiones. [RFMAC-9448]

2107

Novedades

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

Problemas resueltos

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

2106

Novedades

Compatibilidad con direcciones URL personalizadas a través de redirecciones 301

Puede agregar direcciones URL que redirigen a Citrix Workspace desde StoreFront o Citrix Gateway a través de redirecciones HTTP 301.

Si migra de StoreFront a Citrix Workspace, puede redirigir la URL de StoreFront a una URL de Citrix Workspace mediante una redirección HTTP 301. Como resultado, al agregar una URL antigua de StoreFront, se le redirige automáticamente a Citrix Workspace.

Ejemplo de una redirección:

La URL de StoreFront: `https://< Citrix Storefront url>/Citrix/Roaming/Accounts` se puede redirigir a una URL de Citrix Workspace: `https://<Citrix Workspace url>/Citrix/Roaming/Accounts`.

Nota:

- La aplicación Citrix Workspace para Mac no admite la multifrecuencia de doble tono (DTMF) con Microsoft Teams debido a los cambios pendientes de Microsoft.
- A partir de esta versión, es posible que el número de versión de Citrix Viewer y el número de versión de la aplicación Citrix Workspace no coincidan. Este cambio no afecta a su experiencia de usuario.

Continuidad del servicio

La continuidad del servicio elimina o minimiza la dependencia de la disponibilidad de los componentes involucrados en el proceso de conexión. Los usuarios pueden iniciar sus aplicaciones y escritorios virtuales, independientemente del estado de los servicios en la nube.

Para obtener más información, consulte la sección [Continuidad del servicio](#) de la documentación de Citrix Workspace.

Problemas resueltos

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

2104

Novedades

Los usuarios pueden iniciar sesión manualmente en la aplicación Citrix Workspace para Mac para acceder a recursos compartidos de red a menos que la organización haya habilitado Single Sign-On. Para acceder a ubicaciones de red compartidas, abra la aplicación Citrix Workspace, vaya a **Archivos > Recursos compartidos de red** y proporcione sus credenciales. Para obtener más información sobre la configuración de recursos compartidos de red, consulte [Crear y administrar conectores de zonas de almacenamiento](#).

Problemas resueltos

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

2102

Novedades

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

Problemas resueltos

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

2101

Novedades

Chip M1 de silicio de Apple

Ahora, la aplicación Citrix Workspace para Mac es compatible con dispositivos Apple de silicio (chip M1) cuando se utiliza Rosetta 2 en macOS Big Sur (a partir de la versión 11.0). Como resultado, todos los canales virtuales de terceros deben usar Rosetta 2. De lo contrario, es posible que estos canales virtuales no funcionen en la aplicación Citrix Workspace para Mac en macOS Big Sur (a partir de la versión 11.0). Para obtener más información sobre Rosetta, consulte el [artículo de soporte de Apple](#).

Optimización de Microsoft Teams para sesiones de aplicaciones integradas

Ahora, la aplicación Citrix Workspace para Mac admite la optimización de Microsoft Teams para sesiones de aplicaciones integradas. Gracias a ello, puede iniciar Microsoft Teams como una aplicación desde la aplicación Workspace. Para obtener más información, consulte lo siguiente:

- [Optimización para Microsoft Teams](#)
- [Redirección de Microsoft Teams](#)

Multifrecuencia de doble tono (DTMF) con Microsoft Teams

Ahora, la aplicación Citrix Workspace para Mac 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.

Problemas resueltos

- Puede que las reuniones de Microsoft Teams no se abran desde OWA (Outlook Web App), lo que provoca que todas las ventanas relacionadas se cierren inesperadamente. [CTXBR-1175]
- Al iniciar una videollamada, Microsoft Teams puede dejar de responder y mostrar el error `Citrix HDX not connected`. [RFMAC-6727]
- En macOS Big Sur (11.0.1), puede que falle la conexión de dispositivos USB, lo que provoca que la sesión se cierre inesperadamente. [RFMAC-7079]
- En un escritorio publicado, los archivos guardados en el dispositivo Mac local pueden mostrar una fecha de creación de archivos del 30 de noviembre de 1979, en lugar de la fecha actual. [CVADHELP-16309]
- A veces, es posible que la pantalla de inicio de sesión de las aplicaciones publicadas no se muestre correctamente, sino que se muestra en un tamaño de ventana reducido y un color de fondo rojo. [CVADHELP-16027]
- Es posible que las llamadas de audio se desconecten de su lado cuando desconecte y conecte dispositivos de audio. [RFMAC-7371]
- Se copia texto entre aplicaciones de Office 365, incluso cuando la directiva de restricción del portapapeles está habilitada. [CTXBR-1166]
- Puede que Microsoft Teams no se inicie debido a problemas con el motor HDX RealTime Connector y aparezca el siguiente mensaje de error.

`Sorry, we couldn't connect you`

[CVADHELP-16432]

2012

Novedades

Chip M1 de Apple (Tech Preview)

Ahora, la aplicación Citrix Workspace para Mac admite dispositivos con chips M1 de silicio de Apple en una versión Tech Preview.

Optimización para compartir pantalla con Microsoft Teams

Ahora, la optimización para compartir pantalla con Microsoft Teams está disponible en la aplicación Citrix Workspace para Mac. Para obtener más información, consulte lo siguiente:

- [Optimización para Microsoft Teams](#)
- [Redirección de Microsoft Teams](#)

Mejoras en el rendimiento

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

Problemas resueltos

- Al usar la aplicación Citrix Workspace para Mac 2008 o posterior, puede que no inicien varias instancias de una aplicación publicada. [CVADHELP-16019]
- Puede que la redirección de USB genérico no se inicie cuando se utiliza una base de acoplamiento USB. [RFMAC-6687]
- Si intenta abrir una ventana mediante CTRL+O en escritorios publicados, pueden aparecer dos ventanas abiertas. [CVADHELP-15747]
- Al usar la aplicación Citrix Workspace para Mac en la Beta de macOS Big Sur, es posible que las llamadas de audio se desconecten. El problema se produce al desconectar dispositivos de audio y conectar otros dispositivos de audio durante una llamada de audio. [RFMAC-6112]
- Es posible que el motor de HDX RealTime Connector se cierre de forma inesperada al encender y apagar la cámara en Microsoft Teams. [RFMAC-6293]
- Puede que Citrix Files no se inicie desde la aplicación Workspace para Mac debido a problemas con el inicio de sesión único SSO. [RFMAC-4477]

2010

Novedades

Mejora en la autenticación

Para proporcionar una experiencia fluida, ahora el cuadro de diálogo de autenticación aparece dentro de la aplicación Citrix Workspace. Los detalles de la tienda aparecen en la pantalla de inicio de sesión. Los tokens de autenticación se cifran y almacenan para que no tenga que volver a introducir las credenciales en caso de reinicio del sistema o de la sesión.

Nota:

Esta mejora de la autenticación solo se aplica en implementaciones en la nube.

Compatibilidad con macOS Big Sur

La aplicación Citrix Workspace para Mac es compatible con macOS Big Sur (11.0.1).

Mejoras en el rendimiento

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

Problemas resueltos

- Puede que las aplicaciones o los escritorios publicados no se inicien y aparezca un mensaje de error. El problema se produce si el nombre del equipo contiene caracteres especiales. [CVADHELP-15492]
- Puede que no se inicie sesión en aplicaciones y escritorios publicados. El problema se produce cuando utiliza un mouse para hacer clic en **Aceptar** para iniciar sesión. [CVADHELP-15300]

2009

Novedades

Optimización para Microsoft Teams (Tech Preview)

Optimización para Microsoft Teams de escritorio mediante Citrix Virtual Apps and Desktops y la aplicación Citrix Workspace. La optimización para Microsoft Teams es similar a HDX RealTime Optimization para Microsoft Skype Empresarial. La diferencia es que agrupamos todos los componentes necesarios para la optimización de Microsoft Teams en el VDA y en la aplicación Workspace para Mac. La aplicación Citrix Workspace para Mac ofrece audio y vídeo con la optimización de Microsoft Teams.

Para obtener más información, consulte lo siguiente:

- [Optimización para Microsoft Teams](#)
- [Redirección de Microsoft Teams](#)
- Problemas conocidos

Aplicación Citrix Workspace para Mac en la Beta de macOS Big Sur

La aplicación Citrix Workspace 2009 para Mac se ha probado en la Beta 8 de macOS Big Sur. Utilice esta configuración en un entorno de prueba y envíenos sus [comentarios](#). Consulte la sección Problemas conocidos para ver los problemas específicos de la Beta de macOS Big Sur.

Precaución:

No utilice la aplicación Citrix Workspace para Mac en versiones Beta de macOS Big Sur en entornos de producción.

Extensiones de kernel para la redirección de USB

La aplicación Citrix Workspace 2009 para Mac ya no depende de las extensiones de kernel (KEXT) para la redirección de USB.

Problemas resueltos

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

2008

Novedades

Mejoras en el rendimiento

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

Compatibilidad con versiones de macOS

La aplicación Citrix Workspace 2008 para Mac es la última versión que funciona con las versiones High Sierra (10.13) y Mojave (10.14) de macOS.

Problemas resueltos

Si agrega el CLUF en los VDA, es posible que, al iniciar escritorios publicados, vea una pantalla gris o negra. [CVADHELP-14986]

2007

Novedades

Mejoras en el rendimiento

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

Problemas resueltos

- Cuando un usuario habilita Enlightened Data Transport (EDT) en Citrix Gateway, problemas en la configuración de audio del cliente pueden provocar que la aplicación Citrix Workspace para Mac se cierre de forma imprevista. [CVADHELP-14686]
- Cuando se utiliza el SDK de Intel en agentes VDA que tienen habilitada la directiva **Usar códec de vídeo para compresión**, puede aparecer una pantalla de color verde al intentar iniciar escritorios publicados. [CVADHELP-13647]
- Los intentos de obtener los datos de latencia WMI (Instrumental de administración de Windows) pueden fallar en las versiones 2002 y 2005 de la aplicación Citrix Workspace para Mac. [RFMAC-4325]

2006

Novedades

Actualización en Citrix Analytics Service

La aplicación Citrix Workspace está diseñada para transmitir datos de forma segura a Citrix Analytics Service desde sesiones ICA que se inician desde un explorador web. Para obtener más información sobre cómo utiliza esta información Citrix Analytics, consulte [Self-Service for Performance](#) y [Self-service search for Virtual Apps and Desktops](#).

H.264 para la redirección de cámaras web

Ahora la aplicación Citrix Workspace para Mac admite el estándar de compresión de vídeo H.264 (también conocido como MPEG-4 AVC). Como resultado, las aplicaciones publicadas de 64 bits ya pueden usar la redirección de cámaras web.

Mejoras de estabilidad

En esta versión se han resuelto problemas para mejorar la estabilidad general.

Problemas resueltos

- Es posible que no se pueda iniciar sesión en la aplicación Citrix Workspace para Mac, tras lo cual se muestra una interfaz de usuario que no tiene nada que ver. Como solución temporal, haga clic en **Actualizar aplicaciones** en el menú para cargar el almacén. [RFMAC-4063]

Problemas conocidos

Problemas conocidos en la versión 2112

No se han observado nuevos problemas en esta versión.

Problemas conocidos en la versión 2111

No se han observado nuevos problemas en esta versión.

Problemas conocidos en la versión 2109.1

No se han observado nuevos problemas en esta versión.

Problemas conocidos en la versión 2109

- Si configuró la aplicación Workspace mediante el archivo `.cr` e inició sesión con sus credenciales, la página de inicio aparece tras una demora. [RFMAC-9990]
- Si se abre una aplicación web progresiva (PWA) protegida en macOS, no se aplican las directivas de *protección de aplicaciones*. [RFMAC-10128]
- Después de agregar almacenes en la aplicación Workspace, cambiar el **Período de reautenticación actual** en **Período de reautenticación de la aplicación Workspace** y cambiar del almacén local al almacén de la nube unos minutos después, su sesión del almacén de la nube se cierra y aparece un mensaje de autenticación. Una vez que haya iniciado sesión en la aplicación Workspace, el icono giratorio aparece indefinidamente y no puede iniciar sesión. [RFMAC-10140]

Problemas conocidos en la versión 2108.1

No se han observado nuevos problemas en esta versión.

Problemas conocidos en la versión 2108

Al iniciar una aplicación SaaS suscrita después de cambiar el dominio de autenticación en la consola del servidor, la sesión no se inicia y aparece este mensaje de error:

“El dominio de autenticación ha cambiado. Vuelva a iniciar sesión más tarde”. [RFMAC-9616]

Problemas conocidos en la versión 2107

Al cambiar el dominio de autenticación en la consola del servidor e iniciar sesión con sus credenciales, aparece este mensaje de error:

“No se puede conectar con el servidor”

Puede acceder al almacén tras hacer clic en **Aceptar**. [RFMAC-9494]

Problemas conocidos en la versión 2106

Aparece una ventana negra al compartir la pantalla. [HDX-30083]

Problemas conocidos en la versión 2104

No se han observado nuevos problemas en esta versión.

Problemas conocidos en la versión 2102

No se han observado nuevos problemas en esta versión.

Problemas conocidos en la versión 2101

- Es posible que no se pueda acceder a los archivos ubicados en Recursos compartidos de red desde la aplicación Workspace para Mac, incluso aunque la opción esté habilitada. [RFMAC-7272]
- En macOS Big Sur, puede que no se inicie la aplicación web SSO SAML en la aplicación Citrix Workspace para Mac y aparezca el siguiente mensaje de error.

Page could not load. Please **try** again later or contact your administrator **for** assistance. Incident ID:-202

[RFMAC-7282]

Problemas conocidos en la versión 2012

- Al iniciar una videollamada, Microsoft Teams puede dejar de responder y mostrar el error **Citrix HDX not connected**. Como solución temporal, reinicie Microsoft Teams o el VDA. [RFMAC-6727]
- Las videollamadas desde Skype Empresarial de Microsoft no están disponibles en macOS Big Sur (11.0.1).

- En macOS Big Sur (11.0.1), puede que falle la conexión de dispositivos USB, lo que provoca que la sesión se cierre inesperadamente. Como solución temporal, vuelva a conectar el dispositivo USB. [RFMAC-7079]

Problemas conocidos en la versión 2010

- En Skype Empresarial, los vídeos entrantes no se pueden ver en macOS Big Sur (11.0.1).
- Al usar la aplicación Citrix Workspace para Mac 2008 o posterior, puede que no inicien varias instancias de una aplicación publicada. [CVADHELP-16019]
- Puede que la redirección de USB genérico no se inicie cuando se utiliza una base de acoplamiento USB. [RFMAC-6687]
- Al utilizar FaceTime en un MacBook Pro 2018 o una versión más reciente, es posible que los usuarios vean una barra rectangular verde, negra o distorsionada en la parte inferior de la vista previa del vídeo. [RFMAC-2829]

Problemas conocidos en la versión 2009

- Solo se pueden compartir aplicaciones de terceros, como, por ejemplo, Microsoft PowerPoint, al compartir la pantalla en Microsoft Teams desde la aplicación Citrix Workspace para Mac. Sin embargo, los demás usuarios pueden compartir la pantalla sin problema. [RFMAC-3403]
- Al usar la aplicación Citrix Workspace para Mac en la Beta de macOS Big Sur, es posible que las llamadas de audio se desconecten. El problema se produce al desconectar dispositivos de audio y conectar otros dispositivos de audio durante una llamada de audio. [RFMAC-6112]
- Es posible que el motor de HDX RealTime Connector se cierre de forma inesperada al cambiar de dispositivo de cámara en una videollamada optimizada en Microsoft Teams. [RFMAC-6157]
- Es posible que las llamadas de audio y vídeo se desconecten al cambiar de red en Microsoft Teams. [RFMAC-6292]
- En una implementación en la nube, es posible que los escritorios publicados se inicien con un color de fondo diferente. El problema ocurre de forma intermitente en algunas versiones de la Beta de macOS Big Sur. [RFMAC-6343]
- Es posible que falte el icono del instalador de la aplicación Citrix Workspace para Mac al abrir el archivo **CitrixWorkspaceApp.dmg**. El problema ocurre de forma intermitente en algunas versiones de la Beta de macOS Big Sur. [RFMAC-6378]
- Es posible que el motor de HDX RealTime Connector se cierre de forma inesperada al encender y apagar la cámara en Microsoft Teams. [RFMAC-6293]

Problemas conocidos en la versión 2008

No se han observado nuevos problemas en esta versión.

Problemas conocidos en la versión 2007

No se han observado nuevos problemas en esta versión.

Problemas conocidos en la versión 2006

No se han observado nuevos problemas en esta versión.

Avisos legales de terceros

La aplicación Citrix Workspace puede incluir software de terceros con licencias definidas en las condiciones del siguiente documento:

[Aplicación Citrix Workspace para Linux: Avisos de terceros](#)

Requisitos del sistema y compatibilidad

February 11, 2022

Sistemas operativos compatibles

La aplicación Citrix Workspace para Mac es compatible con los siguientes sistemas operativos:

- macOS Monterey (12.0.1)
- macOS Big Sur 11 (incluidos parches y versiones menores)
- macOS Catalina (10.15)

Productos Citrix compatibles

La aplicación Citrix Workspace para Mac es compatible con todas las versiones actualmente admitidas de los siguientes productos Citrix. Para obtener más información acerca de la vida útil de los productos Citrix y para determinar cuándo deja Citrix de ofrecer versiones específicas de los productos, consulte [Citrix Product Lifecycle Matrix](#).

Exploradores compatibles

La aplicación Citrix Workspace para Mac es compatible con los siguientes exploradores web:

- Safari 7.0 y versiones posteriores
- Mozilla Firefox 22.x y versiones posteriores
- Google Chrome 28.x y versiones posteriores

Requisitos de hardware

- 257,7 MB de espacio libre en el disco duro
- Una red o conexión de Internet en uso para conectarse con los servidores

Requisitos de software

- Para implementar la aplicación Citrix Workspace para Mac:
 - La aplicación Citrix Workspace para Web 2.1, 2.5 y 2.6
- StoreFront:
StoreFront 2.x o una versión posterior para el acceso nativo a aplicaciones desde la aplicación Citrix Workspace para Mac o desde un explorador web.

Conexiones, certificados y autenticación

Conexiones

La aplicación Citrix Workspace para Mac admite las conexiones siguientes con Citrix Virtual Apps and Desktops:

- HTTPS
- ICA sobre TLS

La aplicación Citrix Workspace para Mac admite las configuraciones siguientes:

Para conexiones LAN	Para conexiones locales o remotas seguras
StoreFront con un sitio de Citrix Receiver para Web o servicios de StoreFront	Citrix Gateway 10.5-12.0, incluido VPX; Enterprise Edition 9.x-10.x, incluido VPX; VPX

Certificados

Certificados privados (autofirmados)

Si se ha instalado un certificado privado en la puerta de enlace remota, el certificado raíz de la entidad de certificación de la organización debe estar instalado en el dispositivo de usuario. A continuación, puede acceder a los recursos de Citrix mediante la aplicación Citrix Workspace para Mac.

Nota:

Cuando el certificado de la puerta de enlace remota no se puede verificar al conectarse, se muestra un mensaje de advertencia sobre la presencia de un certificado que no es de confianza porque el certificado raíz no está incluido en el almacén de claves local. Cuando un usuario decide ig-

Ignorar la advertencia, se muestra una lista de aplicaciones. Sin embargo, las aplicaciones no se inician.

Importación de certificados raíz en dispositivos con la aplicación Citrix Workspace para Mac

Obtenga el certificado raíz de la autoridad emisora de certificados y envíelo por correo electrónico a una cuenta configurada en el dispositivo. Al seleccionar el adjunto, se le solicitará que importe el certificado raíz.

Certificados comodín

Se usan certificados comodín en lugar de los certificados de servidor individuales para cualquier servidor dentro del mismo dominio. La aplicación Citrix Workspace para Mac admite certificados comodín.

Certificados intermedios con Citrix Gateway

Si la cadena de certificados incluye un certificado intermedio, deberá asignar este certificado al certificado del servidor Citrix Gateway. Para obtener información sobre esta tarea, consulte la documentación de [Citrix Gateway](#). Para obtener más información sobre la instalación, la vinculación y la actualización de certificados, consulte [How to Install and Link Intermediate Certificate with Primary CA on Citrix Gateway](#).

Directiva de validación conjunta de certificados de servidor

Esta versión de la aplicación Citrix Workspace para Mac tiene una directiva más estricta para validar los certificados de servidor.

Importante

Antes de instalar esta versión de la aplicación Citrix Workspace para Mac, confirme que los certificados del servidor o de la puerta de enlace se han configurado correctamente como se describe aquí. Las conexiones pueden fallar si:

- La configuración del servidor o la puerta de enlace incluye un certificado raíz incorrecto
- La configuración del servidor o la puerta de enlace no incluye todos los certificados intermedios
- La configuración del servidor o la puerta de enlace incluye un certificado intermedio caducado o no válido
- La configuración del servidor o la puerta de enlace incluye un certificado intermedio con firmas cruzadas

Cuando valida un certificado de servidor, la aplicación Citrix Workspace para Mac usa ahora **todos** los certificados suministrados por el servidor (o la puerta de enlace) para validarlo. Al igual que en

las versiones anteriores, esta versión de la aplicación Citrix Workspace para Mac también comprueba posteriormente que los certificados son de confianza. Si no todos los certificados son de confianza, la conexión falla.

Esta directiva es más estricta que la directiva de certificados presente en los exploradores web. Muchos exploradores web incluyen un gran conjunto de certificados raíz en los que confían.

El servidor (o la puerta de enlace) debe estar configurado con el conjunto correcto de certificados. Un conjunto incorrecto de certificados puede provocar que falle la conexión de la aplicación Citrix Workspace para Mac.

Supongamos que se configura una puerta de enlace con estos certificados válidos. Esta configuración se recomienda para los clientes que requieren una validación más estricta, que necesitan determinar exactamente cuál es el certificado raíz usa la aplicación Citrix Workspace para Mac:

- “Ejemplo de certificado de servidor”
- “Ejemplo de certificado intermedio”
- “Ejemplo de certificado raíz”

A continuación, la aplicación Citrix Workspace para Mac comprueba que todos los certificados sean válidos. La aplicación Citrix Workspace para Mac también comprueba que ya confía en “Ejemplo de certificado raíz”. Si la aplicación Citrix Workspace para Mac no confía en “Ejemplo de certificado raíz”, la conexión falla.

Importante

Algunas entidades de certificación tienen más de un certificado raíz. Si necesita usar esta validación más estricta, compruebe que la configuración usa el certificado raíz correspondiente. Por ejemplo, actualmente hay dos certificados (“DigiCert”/”GTE CyberTrust Global Root” y “DigiCert Baltimore Root”/”Baltimore CyberTrust Root”) que pueden validar los mismos certificados de servidor. En algunos dispositivos de usuario, están disponibles ambos certificados raíz. En otros dispositivos, solo uno está disponible (“DigiCert Baltimore Root” o “Baltimore CyberTrust Root”). Si configura “GTE CyberTrust Global Root” en la puerta de enlace, fallan las conexiones de la aplicación Citrix Workspace para Mac en esos dispositivos de usuario. Consulte la documentación de la entidad de certificación para determinar qué certificado raíz debe usarse. Los certificados raíz también caducan, como todos los demás certificados.

Nota

Algunos servidores y puertas de enlace nunca envían el certificado raíz, aunque se haya configurado. En esos casos, esta validación más estricta no es posible.

Supongamos ahora que se configura una puerta de enlace con estos certificados válidos. Esta configuración, sin certificado raíz, es la que se suele recomendar:

- “Ejemplo de certificado de servidor”
- “Ejemplo de certificado intermedio”

La aplicación Citrix Workspace para Mac usa esos dos certificados. Luego, busca un certificado raíz en el dispositivo del usuario. Si encuentra un certificado de confianza que se valida correctamente, como “Ejemplo de certificado raíz”, la conexión se realiza correctamente. De lo contrario, la conexión falla. Esta configuración proporciona el certificado intermedio que necesita la aplicación Citrix Workspace para Mac, pero también permite que la aplicación Citrix Workspace para Mac elija cualquier certificado raíz válido y de confianza.

Supongamos ahora que se configura una puerta de enlace con estos certificados:

- “Ejemplo de certificado de servidor”
- “Ejemplo de certificado intermedio”
- “Certificado raíz incorrecto”

Un explorador web podría ignorar el certificado raíz incorrecto. No obstante, la aplicación Citrix Workspace para Mac no ignora el certificado raíz incorrecto y la conexión falla.

Algunas entidades de certificación usan más de un certificado intermedio. En este caso, la puerta de enlace se configura normalmente con todos los certificados intermedios (pero sin el certificado raíz):

- “Ejemplo de certificado de servidor”
- “Ejemplo de certificado intermedio 1”
- “Ejemplo de certificado intermedio 2”

Importante

Algunas entidades de certificación utilizan un certificado intermedio con firmas cruzadas, diseñado para situaciones en las que hay más de un certificado raíz. Un certificado raíz anterior sigue en uso al mismo tiempo que un certificado raíz posterior. En este caso, hay al menos dos certificados intermedios. Por ejemplo, el certificado raíz anterior “Class 3 Public Primary Certification Authority” tiene el certificado intermedio correspondiente de firmas cruzadas “Verisign Class 3 Public Primary Certification Authority - G5”. No obstante, un certificado raíz posterior correspondiente “Verisign Class 3 Public Primary Certification Authority - G5” también está disponible y reemplaza a “Class 3 Public Primary Certification Authority”. El certificado raíz posterior no usa ningún certificado intermedio con firmas cruzadas.

Nota

El certificado intermedio con firmas cruzadas y el certificado raíz tienen el mismo Nombre de sujeto (Emitido para), pero el certificado intermedio con firmas cruzadas tiene otro Nombre de emisor (Emitido por). Esto distingue el certificado intermedio con firmas cruzadas de un certificado intermedio normal (como “Certificado intermedio 2 - ejemplo”).

Esta configuración, sin certificado raíz y sin certificado intermedio con firmas cruzadas, es la que se suele recomendar:

- “Ejemplo de certificado de servidor”
- “Ejemplo de certificado intermedio”

No configure la puerta de enlace para que use el certificado intermedio con firmas cruzadas, porque selecciona el certificado raíz anterior:

- “Ejemplo de certificado de servidor”
- “Ejemplo de certificado intermedio”
- “Ejemplo de certificado intermedio con firmas cruzadas” [no recomendado]

No se recomienda configurar la puerta de enlace solamente con el certificado del servidor:

- “Ejemplo de certificado de servidor”

En este caso, si la aplicación Citrix Workspace para Mac no puede localizar todos los certificados intermedios, la conexión falla.

Autenticación

Para conexiones con StoreFront, la aplicación Citrix Workspace para Mac admite los siguientes métodos de autenticación:

	Workspace para Web con exploradores	Sitio de servicios StoreFront (nativo)	Sitio de servicios XenApp de StoreFront (nativo)	Citrix Gateway en Citrix Workspace para Web (explorador)	Citrix Gateway en el sitio de StoreFront Services (nativo)
Anónimo	Sí	Sí			
Dominio	Sí	Sí		Sí*	Sí*
PassThrough de dominio					
Token de seguridad				Sí*	Sí*
Autenticación de dos factores (dominio con token de seguridad)				Sí*	Sí*
SMS				Sí*	Sí*
Tarjeta inteligente	Sí	Sí		Sí*	Sí

		Sitio de servicios XenApp de StoreFront (nativo)	Sitio de servicios StoreFront (nativo)	Citrix Gateway en Citrix Workspace para Web (explorador)	Citrix Gateway en el sitio de StoreFront Services (nativo)
Certificado de usuario	Workspace para Web con exploradores	Sitio de servicios StoreFront (nativo)	Sitio de servicios XenApp de StoreFront (nativo)	Sí	Sí (plug-in de Citrix Gateway)

*Disponible solo en implementaciones que incluyen Citrix Gateway, con o sin el plug-in asociado instalado en el dispositivo.

Instalación, desinstalación y actualización

February 11, 2022

La aplicación Citrix Workspace para Mac contiene un solo paquete de instalación y admite el acceso remoto a través de Citrix Gateway y Secure Web Gateway.

Puede instalar la aplicación Citrix Workspace para Mac de cualquiera de las siguientes maneras:

- Desde el sitio web de Citrix.
- Automáticamente desde Workspace para Web.
- Mediante una herramienta de distribución electrónica de software (ESD).

Instalación manual

Desde Citrix.com (instalación de usuario)

Si es la primera vez que utiliza la aplicación Citrix Workspace para Mac, puede descargarla desde Citrix.com o desde su propio sitio de descargas. A continuación, para configurar una cuenta, introduzca una dirección de correo electrónico en lugar de una dirección URL de servidor. La aplicación Citrix Workspace para Mac determina el dispositivo Citrix Gateway o el servidor de StoreFront asociados a la dirección de correo electrónico. A continuación, solicita al usuario que inicie sesión y continúe con la instalación. Esta función se conoce como detección de cuentas basada en correo electrónico.

Nota:

Un usuario nuevo es un usuario que no tiene la aplicación Citrix Workspace para Mac instalada en su dispositivo.

La detección de cuentas basada en correo electrónico para un usuario nuevo no se aplica cuando la aplicación se descarga desde una ubicación distinta a Citrix.com (por ejemplo, un sitio de Citrix Receiver para Web).

Si el sitio requiere la configuración de la aplicación Citrix Workspace para Mac, utilice un método de implementación alternativo.

Mediante una herramienta de distribución electrónica de software (ESD)

Un usuario que utiliza la aplicación Citrix Workspace para Mac por primera vez debe introducir una dirección URL de servidor para configurar una cuenta.

Desde la página Descargas de Citrix

Puede instalar la aplicación Citrix Workspace para Mac desde un recurso compartido de red o directamente en el dispositivo del usuario. Para instalar la aplicación, descargue el archivo desde el sitio web [Descargas](#) de Citrix.

Para instalar la aplicación Citrix Workspace para Mac:

1. Descargue el archivo DMG para la versión de la aplicación Citrix Workspace para Mac que quiere instalar desde el sitio web de Citrix.
2. Abra el archivo descargado.
3. En la página Introducción, haga clic en **Continuar**.
4. En la página **Licencia**, haga clic en **Continuar**.
5. Haga clic en **Aceptar** para aceptar los términos del contrato de licencia.
6. En la página **Tipo de instalación**, haga clic en **Instalar**.
7. En la página **Agregar cuenta**, seleccione **Agregar cuenta** y, a continuación, haga clic en **Continuar**.
8. Introduzca el nombre de usuario y la contraseña de un administrador del dispositivo local.

Desinstalación

Para desinstalar manualmente la aplicación Citrix Workspace para Mac, abra el archivo DMG. Seleccione **Desinstalar aplicación Citrix Workspace** y siga las instrucciones que aparecen en pantalla. El archivo DMG es el archivo que se descarga desde Citrix al instalar la aplicación Citrix Workspace para Mac por primera vez. Si el archivo ya no está en el equipo, vuelva a descargarlo de [Descargas de Citrix](#) para desinstalar la aplicación.

Actualizar

La aplicación Citrix Workspace para Mac le envía notificaciones cuando hay una actualización disponible de una versión existente o una actualización a una versión más reciente.

Puede actualizar la versión de su aplicación Citrix Workspace para Mac desde cualquiera de las versiones anteriores de la aplicación Citrix Workspace para Mac.

Al actualizar la versión de la aplicación Citrix Workspace para Mac a una más reciente, la versión anterior se desinstala automáticamente. No es necesario reiniciar la máquina.

Update

February 21, 2022

Actualización manual

Para actualizar manualmente la aplicación Citrix Workspace para Mac, descargue e instale la versión más reciente de la aplicación desde la página [Descargas de Citrix](#).

Actualización automática

Cuando se publica una nueva versión de la aplicación Citrix Workspace, Citrix envía una actualización al sistema que tiene instalada la aplicación Citrix Workspace. Recibirá una notificación cuando la actualización esté disponible.

Nota:

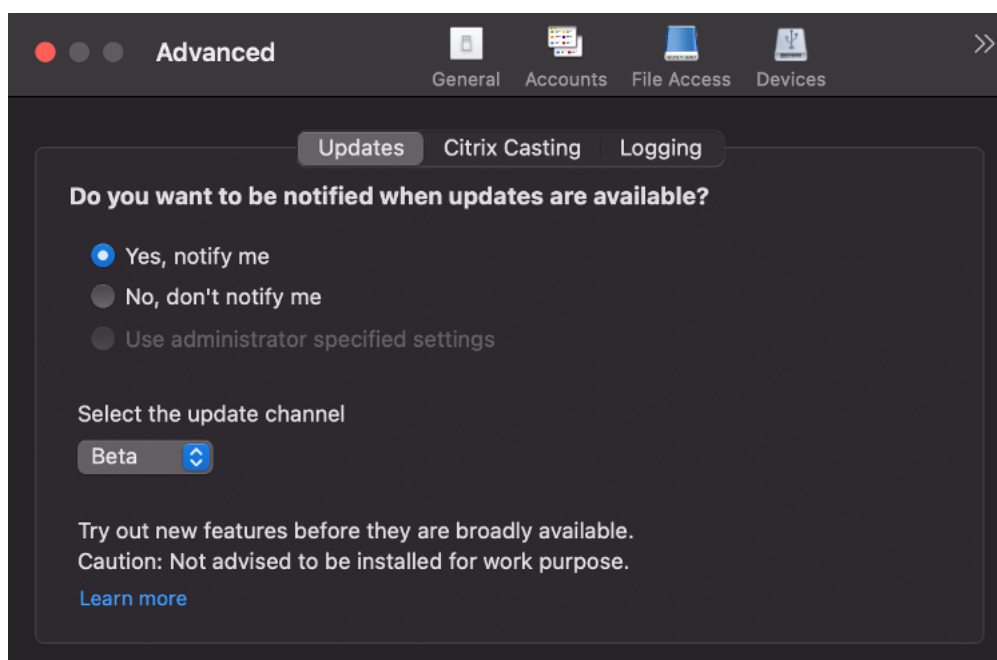
- Si configuró un proxy SSL interceptor de salida, agregue una excepción al servicio de firma de actualización automática de Workspace <https://citrixupdates.cloud.com/> y a la ubicación de descarga <https://downloadplugins.citrix.com/> para recibir actualizaciones de Citrix.
- El sistema debe tener una conexión a Internet para recibir actualizaciones.
- Los usuarios de Workspace para Web no pueden descargar automáticamente la directiva de StoreFront.
- Citrix HDX RTME para macOS se incluye en Actualizaciones de Citrix Workspace. Se le notifica sobre la actualización de HDX RTME disponible en la aplicación Citrix Workspace.
- A partir de la versión 2111, se modifican las rutas de registros de Actualizaciones de Citrix Workspace. Los registros de actualizaciones de Workspace se hallan en `/Library/Logs`

/Citrix Workspace Updater. Para obtener información sobre la recopilación de registros, consulte la sección Recopilación de registros.

Instalar el programa Beta de la aplicación Citrix Workspace

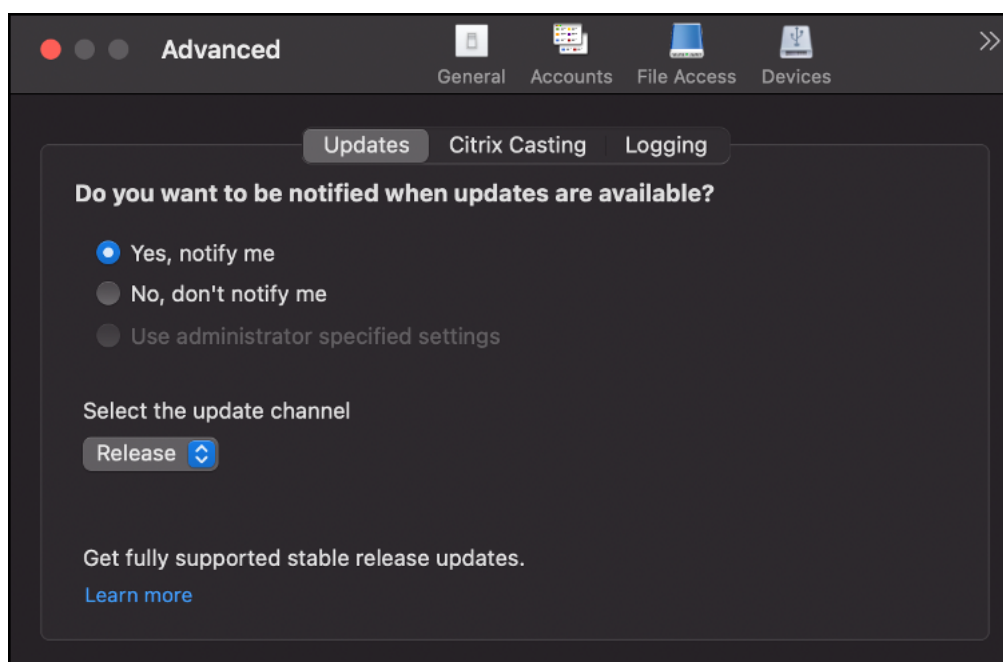
Recibirá una notificación de actualización cuando la Citrix Workspace se haya configurado para obtener actualizaciones automáticas. Para instalar la compilación Beta en el sistema, siga estos pasos:

1. Abra la aplicación Citrix Workspace.
2. Haga clic con el botón secundario en Citrix Workspace, en la barra de herramientas, y haga clic en **Preferencias > Avanzado**.
3. Seleccione **Beta** en la lista desplegable cuando la compilación Beta esté disponible.



Para cambiar de una compilación Beta a una compilación pública, siga estos pasos:

1. Abra la aplicación Citrix Workspace.
2. Haga clic con el botón secundario en Citrix Workspace, en la barra de herramientas, y haga clic en **Preferencias > Avanzado**.
3. Seleccione **Público** en la lista desplegable **Seleccione el canal de actualización**.



Nota:

Las compilaciones beta están disponibles para que los clientes las prueben en sus entornos de producción limitados o en entornos que no son de producción y para compartir comentarios. Citrix no acepta casos de asistencia de compilaciones beta, pero agradece [comentarios](#) para mejorarlas. Citrix puede o no actuar a partir de los comentarios en función de su gravedad e importancia. No es aconsejable implementar compilaciones beta en entornos de producción.

Configuración avanzada para actualizaciones automáticas (Actualizaciones de Citrix Workspace)

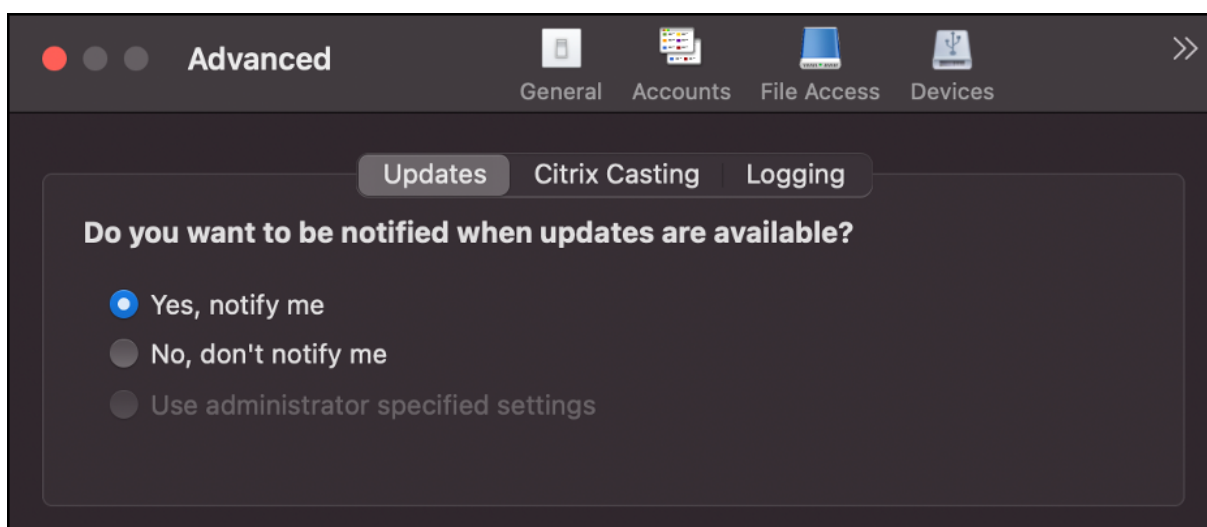
Puede configurar Actualizaciones de Citrix Workspace con estos métodos:

1. Interfaz gráfica (GUI)
2. StoreFront

Configurar las actualizaciones de Citrix Workspace mediante la interfaz gráfica de usuario

Los usuarios pueden supeditar el parámetro de actualizaciones de Citrix Workspace mediante el cuadro de diálogo **Preferencias avanzadas**, que es una configuración por usuario y cuyos parámetros se aplican solamente al usuario actual. Para configurar la actualización mediante la interfaz gráfica de usuario, siga estos pasos:

1. Seleccione el icono de ayuda de la aplicación Citrix Workspace de su Mac.
2. En la lista desplegable, seleccione **Preferencias > Avanzado**.
3. Seleccione la preferencia de las notificaciones de actualización y cierre la ventana.



Configurar Actualizaciones de Citrix Workspace mediante StoreFront

1. Utilice un editor de texto para abrir el archivo `web.config`, que normalmente se encuentra en `C:\inetpub\wwwroot\Citrix\Roaming directory`.
2. Localice el elemento de la cuenta de usuario en el archivo (Store es el nombre de cuenta de la implementación).

Por ejemplo: `<account id=... name="Store">`

Antes de la etiqueta `</account>`, vaya a las propiedades de esa cuenta de usuario:

```
1 <properties>
2     <clear/>
3 </properties>
4 <!--NeedCopy-->
```

3. Agregue la etiqueta de actualización automática después de `<clear />`.

```
1 <account>
2
3     <clear />
4
5     <account id="d1197d2c-ac82-4f13-9346-2ee14d4b0202" name="
6         F84Store"
7         description="" published="true" updaterType="Citrix"
            remoteAccessType="None">
```

```
8
9     <annotatedServices>
10
11     <clear />
12
13     <annotatedServiceRecord serviceRef="1__Citrix_F84Store">
14
15     <metadata>
16
17     <plugins>
18
19     <clear />
20
21     </plugins>
22
23     <trustSettings>
24
25     <clear />
26
27     </trustSettings>
28
29     <properties>
30
31     <property name="Auto-Update-Check" value="auto" />
32
33     <property name="Auto-Update-DeferUpdate-Count" value
34     = "1" />
35
36     <property name="Auto-Update-Rollout-Priority" value=
37     "fast" />
38
39     </properties>
40
41     </metadata>
42
43     </annotatedServiceRecord>
44
45 </annotatedServices>
46
47 <metadata>
48
49 <plugins>
50
51 <clear />
```

```
51     </plugins>
52
53     <trustSettings>
54
55         <clear />
56
57     </trustSettings>
58
59     <properties>
60
61         <clear />
62
63     </properties>
64
65 </metadata>
66
67 </account>
68
69 <!--NeedCopy-->
```

El significado de las propiedades y sus posibles valores se detallan a continuación:

- **Auto-update-Check:** Indica que la aplicación Citrix Workspace detecta automáticamente cuándo hay una actualización disponible.
- **Auto-Update-Rollout-Priority:** Indica el período de entrega en el que puede recibir la actualización.
- **Auto-update-DeferUpdate-Count:** Indica las veces que puede aplazar las notificaciones relativas a las actualizaciones de la versión.

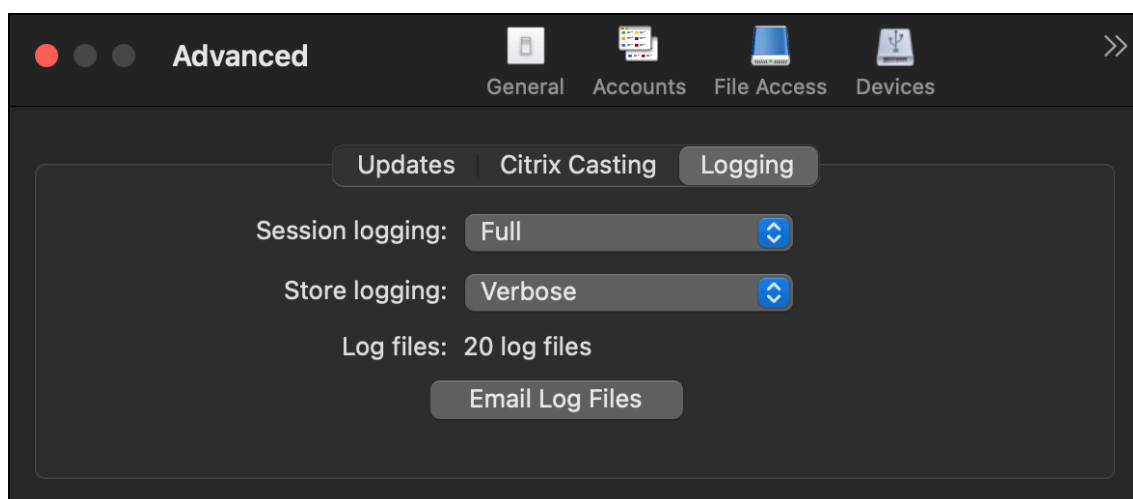
Recopilación de registros

La recopilación de registros simplifica el proceso de recopilación de registros para la aplicación Citrix Workspace. Los registros ayudan a Citrix a solucionar problemas y, en el caso de problemas complicados, facilitan la asistencia técnica.

Puede recopilar registros mediante la interfaz gráfica de usuario.

Recopilación de registros:

1. Abra la aplicación Citrix Workspace.
2. Haga clic con el botón secundario en Citrix Workspace, en la barra de herramientas, y haga clic en **Preferencias > Avanzado**.
3. Selecciona **Registros**.



4. Seleccione uno de estos niveles de registros:

- **Inhabilitado (valor predeterminado):** Se recopilan registros mínimos para la solución de problemas básicos.
- **Diagnósticos de conexión:** Identifica errores durante la conexión. Todos los registros están habilitados hasta el momento en que la sesión se considera correcta.
- **Completo:** Captura todo, incluidos los diagnósticos de conexión. Una vez habilitado, la aplicación Citrix Workspace almacenará hasta 10 registros de sesión; después, se eliminarán empezando por el más antiguo para mantener 10 registros.

Nota:

La selección de la opción de registros **Completo** puede afectar al rendimiento y solo debe usarse al solucionar problemas debidos a la cantidad de datos. No habilite los registros completos durante el uso normal. Al habilitar este nivel de registros, se activa un cuadro de diálogo de advertencia que debe aceptarse para que pueda continuar.

5. Seleccione uno de estos niveles de registros de almacén:

- **Inhabilitado (valor predeterminado):** Se recopilan registros mínimos para la solución de problemas básicos.
- **Normal:** Solo se recopilan registros de comunicación de almacén.
- **Detallado:** Se recopilan registros detallados de autenticación y comunicación de almacén.

6. Haga clic en **Enviar archivos de registros** para recopilar y compartir registros como un archivo ZIP.

Configuración

February 21, 2022

Una vez instalado el software de la aplicación Citrix Workspace para Mac, los usuarios pueden seguir estos pasos de configuración para acceder a sus aplicaciones y escritorios alojados:

Los usuarios podrían conectarse desde Internet o desde ubicaciones remotas. Para esos usuarios, configure la autenticación a través de Citrix Gateway.

Tareas y aspectos relevantes para administradores

En este artículo se describen las tareas y los aspectos que son relevantes para los administradores de la aplicación Citrix Workspace para Mac.

Importante:

Si usa macOS 10.15, asegúrese de que el sistema cumpla con [los requisitos de Apple para los certificados de confianza en macOS 10.15](#). Realice esta comprobación antes de actualizar la versión de la aplicación Citrix Workspace para Mac a la versión 2106.

Administrar marcas de función

Si se produce un problema con la aplicación Citrix Workspace en producción, podemos inhabilitar de manera dinámica una función afectada en la aplicación Citrix Workspace aunque dicha función ya se haya publicado. Para ello, se utilizan marcas de función y un servicio externo denominado LaunchDarkly.

No es necesario que realice ninguna configuración para permitir el tráfico a LaunchDarkly, salvo si tiene un firewall o proxy bloqueando el tráfico saliente. En ese caso, puede habilitar el tráfico a LaunchDarkly a través de direcciones URL o direcciones IP específicas, según sus requisitos de directiva.

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

Permitir el tráfico a las siguientes URL

- events.launchdarkly.com
- stream.launchdarkly.com
- clientstream.launchdarkly.com
- [Firehose.launchdarkly.com](https://firehose.launchdarkly.com)
- mobile.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 asegurarse de 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](#).

Requisitos del sistema para LaunchDarkly

Compruebe que las aplicaciones pueden comunicarse con los siguientes servicios si el parámetro de túnel dividido está **desactivado** en Citrix ADC para estos servicios:

- Servicio de LaunchDarkly.
- Servicio de escucha de APNs

Integración de Content Collaboration Service

Citrix Content Collaboration le permite intercambiar documentos de forma fácil y segura, enviar documentos grandes por correo electrónico, manejar de forma segura transferencias de documentos a terceros y acceder a un espacio de colaboración.

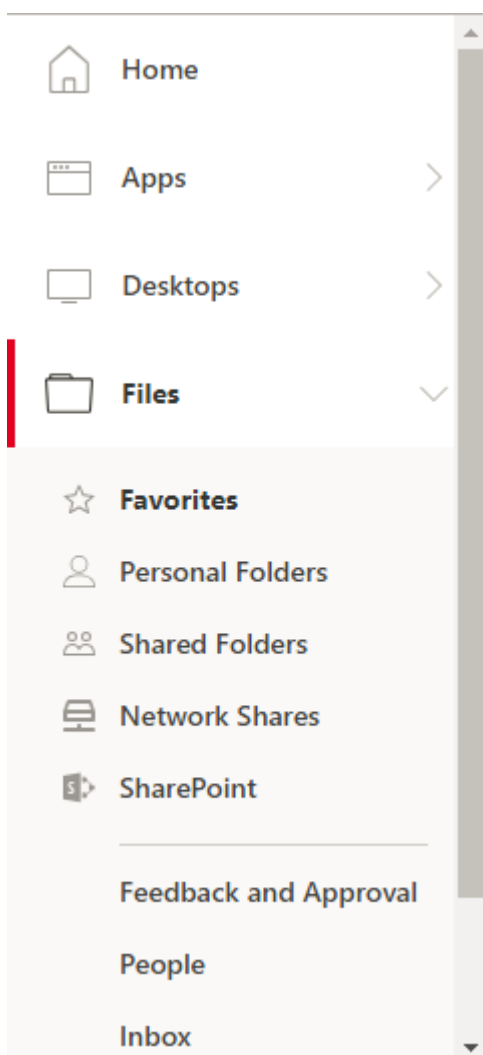
Citrix Content Collaboration ofrece muchas maneras de trabajar, incluida una interfaz web, clientes móviles, aplicaciones de escritorio e integración con Microsoft Outlook y Gmail.

Puede acceder a la funcionalidad Citrix Content Collaboration desde la aplicación Citrix Workspace. Para ello, vaya a la ficha **Archivos** que aparece en la aplicación Citrix Workspace. La ficha **Archivos** solo se ve si Content Collaboration está habilitado en la configuración de Workspace, en la consola de Citrix Cloud.

Nota:

Windows Server 2012 y Windows Server 2016 no permiten la integración de Citrix Content Collaboration debido a una opción de seguridad establecida en el sistema operativo.

En la imagen siguiente se muestra el contenido de ejemplo de la ficha **Archivos** de la nueva aplicación Citrix Workspace:



Limitaciones

- Restablecer la aplicación Citrix Workspace no hace que se cierre la sesión de Citrix Content Collaboration.
- Cambiar de almacén en la aplicación Citrix Workspace no hace que Citrix Content Collaboration cierre la sesión.

Redirección de USB

La redirección de dispositivos USB de HDX permite redirigir dispositivos USB hacia y desde un dispositivo de usuario. Un usuario puede conectar una unidad flash a un equipo local y acceder a ella de forma remota desde un escritorio virtual o desde una aplicación alojada en el escritorio.

Durante una sesión, los usuarios pueden conectar y reproducir dispositivos, incluidos los dispositivos con protocolo de transferencia de imágenes (PTP). Por ejemplo:

- Cámaras digitales, dispositivos con protocolo de transferencia multimedia (MTP) como reproductores de audio digital o reproductores multimedia portátiles
- Dispositivos de punto de venta (POS) y otros dispositivos como cursores SpaceMouse 3D, escáneres, paneles de firmas...

Nota:

El doble salto de USB no se ofrece en sesiones de aplicaciones alojadas en escritorios.

La redirección de USB está disponible para los siguientes:

- Windows
- Linux
- Mac

De manera predeterminada, se permite la redirección de USB para ciertas clases de dispositivos USB, y se rechaza para otras. Para restringir los tipos de dispositivos USB disponibles para un escritorio virtual, actualice la lista de dispositivos USB compatibles con la redirección. Más adelante en esta sección se proporciona más información.

Sugerencia

Cuando se necesite una separación de seguridad entre el dispositivo del usuario y el servidor, asegúrese de informar a los usuarios sobre los tipos de dispositivos USB que deben evitar.

Hay canales virtuales optimizados disponibles para redirigir los dispositivos USB utilizados con más frecuencia y proporcionar un rendimiento superior y mayor eficiencia del ancho de banda sobre redes WAN. Los canales virtuales optimizados suelen ser la mejor opción, especialmente en entornos de alta latencia.

Nota:

A efectos de redirección de USB, la aplicación Citrix Workspace para Mac gestiona los paneles SMART igual que un mouse.

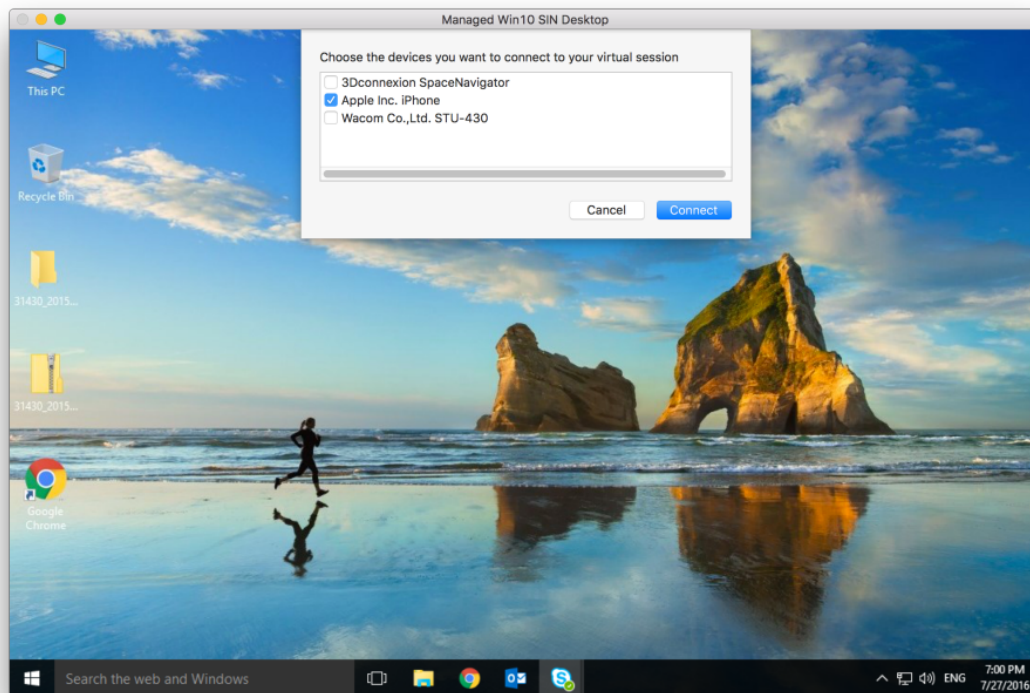
El producto ofrece canales virtuales optimizados para dispositivos USB 3.0 y puertos USB 3.0. Por ejemplo, un canal virtual CDM se utiliza para ver archivos en una cámara o para proporcionar audio a unos auriculares. El producto también admite la redirección de USB genérico de dispositivos USB 3.0 conectados a puertos USB 2.0.

Es posible que algunas funciones avanzadas específicas del dispositivo, como los botones del dispositivo de interfaz humana (HID) de una cámara web, no funcionen como se esperaba con el canal virtual optimizado. Use el canal virtual USB genérico como alternativa.

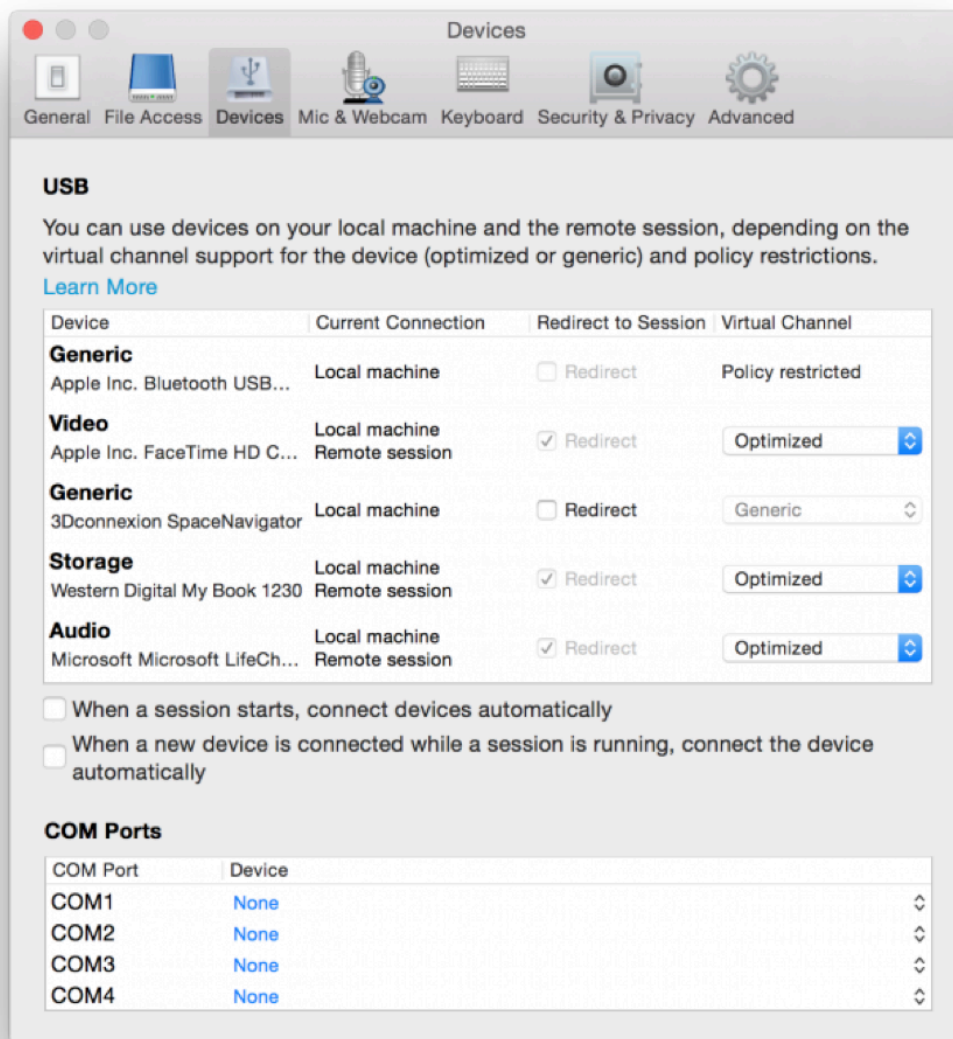
Algunos dispositivos no se redirigen de manera predeterminada y solo están disponibles en la sesión local. Por ejemplo, no sería adecuado redirigir una tarjeta de interfaz de red que está conectada directamente por USB interno.

Para usar la redirección de USB:

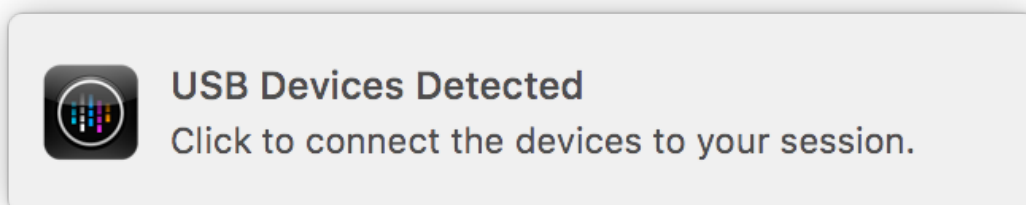
1. Conecte el dispositivo USB al dispositivo donde está instalada la aplicación Citrix Workspace para Mac.
2. Se le pedirá que seleccione los dispositivos USB disponibles en el sistema local.



3. Seleccione el dispositivo que quiere conectar y haga clic en **Conectar**. Si la conexión falla, aparece un mensaje de error.
4. El dispositivo USB aparecerá listado en el panel USB, en la ventana **Preferencias**, en la ficha **Dispositivos**:



5. Seleccione el tipo de canal virtual (Genérico u Optimizado) para el dispositivo USB.
6. Aparecerá un mensaje. Haga clic para conectar el dispositivo USB a su sesión:



Usar y quitar dispositivos USB

Los usuarios pueden conectar un dispositivo USB antes o después de iniciar una sesión virtual. Cuando se usa la aplicación Citrix Workspace para Mac, ocurre lo siguiente:

- Los dispositivos conectados después haber iniciado la sesión aparecen inmediatamente en el menú USB de Desktop Viewer.
- Si un dispositivo USB no se redirige correctamente, a veces se puede resolver el problema esperando para conectar el dispositivo hasta después de que la sesión virtual se ha iniciado.
- Para evitar la pérdida de datos, use el menú de Windows **Extracción segura** antes de quitar el dispositivo USB.

Dispositivos USB admitidos

Después de que Apple anunciara la retirada de las extensiones del kernel (KEXT), la aplicación Citrix Workspace para Mac migró al nuevo marco para dispositivos USB en modo usuario `IOUSBHost` proporcionado por Apple. En este artículo se indican los dispositivos USB compatibles.

Dispositivos USB compatibles con la redirección de USB

Estos dispositivos USB funcionan totalmente con la redirección de USB:

- 3Dconnexion SpaceMouse
- Dispositivos de almacenamiento masivo
- Unidad flash USB Kingston DataTraveler
- Unidad de disco duro externa Seagate
- Unidad flash Kingston/Transcend de 32 GB/64 GB
- Lector/tarjeta inteligente PIV de NIST
- YubiKey

Dispositivos USB que no funcionan con la redirección de USB

Este dispositivo no es compatible con la redirección de USB:

- Disco duro externo SSD Transcend

Dispositivos USB no verificados

Hay muchos dispositivos, no verificados por Citrix, para una redirección de USB correcta con la aplicación Citrix Workspace para Mac. He aquí algunos de estos dispositivos:

- Otros discos duros
- Teclas especiales en el teclado y auriculares que utilizan un protocolo HID personalizado

Compatibilidad con dispositivos de almacenamiento masivo

Hemos visto que no todos los tipos de dispositivos de almacenamiento masivo se pueden redirigir correctamente. Para los dispositivos en los que la redirección falla, existe un canal virtual optimizado denominado Asignación de unidades del cliente. Mediante Asignación de unidades del cliente, el acceso a los dispositivos de almacenamiento masivo se puede controlar mediante las directivas del Delivery Controller.

Compatibilidad con dispositivos isócronos

La redirección de USB genérico no admite la clase isócrona de dispositivos USB en la aplicación Citrix Workspace para Mac. El modo isócrono de transferencia de datos en la especificación de USB indica dispositivos que transmiten los datos con marca de hora a una velocidad constante. Por ejemplo: cámaras web, auriculares USB, etc.

Compatibilidad con dispositivos compuestos

Un dispositivo USB compuesto es un solo dispositivo que puede realizar más de una función. Por ejemplo: impresoras multifunción, iPhone, etc. Por ahora, la aplicación Citrix Workspace para Mac no admite la redirección de dispositivos compuestos a la sesión de Citrix Virtual Apps and Desktops.

Alternativas para dispositivos USB no compatibles

Hay canales virtuales optimizados que pueden gestionar dispositivos que no son compatibles con la redirección de USB genérico. Estos canales virtuales están optimizados para obtener velocidad en comparación con la redirección de USB genérico. He aquí algunos ejemplos:

- **Redirección de cámaras web:** Optimizada para el tráfico de cámaras web sin procesar. El pack de optimización de Microsoft Teams tiene su propio método de redirección de cámaras web. Por lo tanto, no le pertoca el canal virtual de redirección de cámaras web.
- **Redirección de audio:** Optimizada para las transmisiones de audio.
- **Asignación de unidades del cliente:** Optimizada para redirigir dispositivos de almacenamiento masivo a la sesión de Citrix Virtual Apps and Desktops. Por ejemplo: unidades flash, discos duros, DVD-ROM/RW, etc.

Enlightened Data Transport (EDT)

De manera predeterminada, EDT está habilitado en la aplicación Citrix Workspace para Mac.

La aplicación Citrix Workspace para Mac lee los parámetros de **EDT** según están definidos en el archivo `default.ica` y los aplica.

Para inhabilitar EDT, ejecute este comando en un terminal:

```
defaults write com.citrix.receiver.nomas HDXOverUDPAllowed -bool NO
```

Fiabilidad de la sesión y reconexión automática de clientes

Cuando la conectividad de red se ve interrumpida, la fiabilidad de la sesión mantiene las sesiones activas y en la pantalla del usuario. Los usuarios siguen viendo la aplicación que están utilizando hasta que vuelve la conexión.

Con la función de fiabilidad de la sesión, la sesión permanece activa en el servidor. Para indicar que se ha perdido la conectividad, la pantalla del usuario se congela hasta que se recupera la conectividad. La función Fiabilidad de la sesión vuelve a conectar a los usuarios sin pedirles que repitan la autenticación.

Importante

- Los usuarios de la aplicación Citrix Workspace para Mac no pueden anular la configuración del servidor.
- Con la fiabilidad de la sesión habilitada, el puerto predeterminado para la comunicación de la sesión cambia de 1494 a 2598.

Puede usar la función de fiabilidad de la sesión con Transport Layer Security (TLS).

Nota

TLS cifra solo los datos enviados entre el dispositivo de usuario y Citrix Gateway.

Uso de directivas de fiabilidad de la sesión

La configuración de directiva **conexiones de fiabilidad de la sesión** permite o impide la fiabilidad de la sesión.

La configuración de directiva de **tiempo de espera de fiabilidad de la sesión** tiene un tiempo predeterminado de 180 segundos, o tres minutos. Aunque puede ampliar el tiempo en que la fiabilidad de la sesión mantiene abierta una sesión, esta función es práctica para el usuario. Por lo tanto, no pide al usuario que vuelva a autenticarse.

Sugerencia

Es posible que, al prolongar los tiempos de espera de fiabilidad de la sesión, los usuarios se distraigan y se alejen del dispositivo, lo que deja la sesión accesible a usuarios no autorizados.

De forma predeterminada, las conexiones entrantes de fiabilidad de la sesión utilizan el puerto 2598 a menos que cambie el número de puerto definido en la configuración de directiva Número de puerto para fiabilidad de la sesión.

Puede definir la configuración de la directiva **Autenticación para reconexión automática de clientes** de manera que solicite a los usuarios que repitan la autenticación cuando vuelvan a conectarse a las sesiones interrumpidas.

Si usa tanto la fiabilidad de la sesión como la reconexión automática de clientes, las dos actúan de manera secuencial. La fiabilidad de la sesión cierra o desconecta la sesión de usuario después de transcurrido el tiempo que se especifica en la configuración de directiva **Tiempo de espera de fiabilidad de la sesión**. A continuación, se aplicará la configuración de directiva de Reconexión automática de clientes y se intentará reconectar al usuario con la sesión desconectada.

Nota

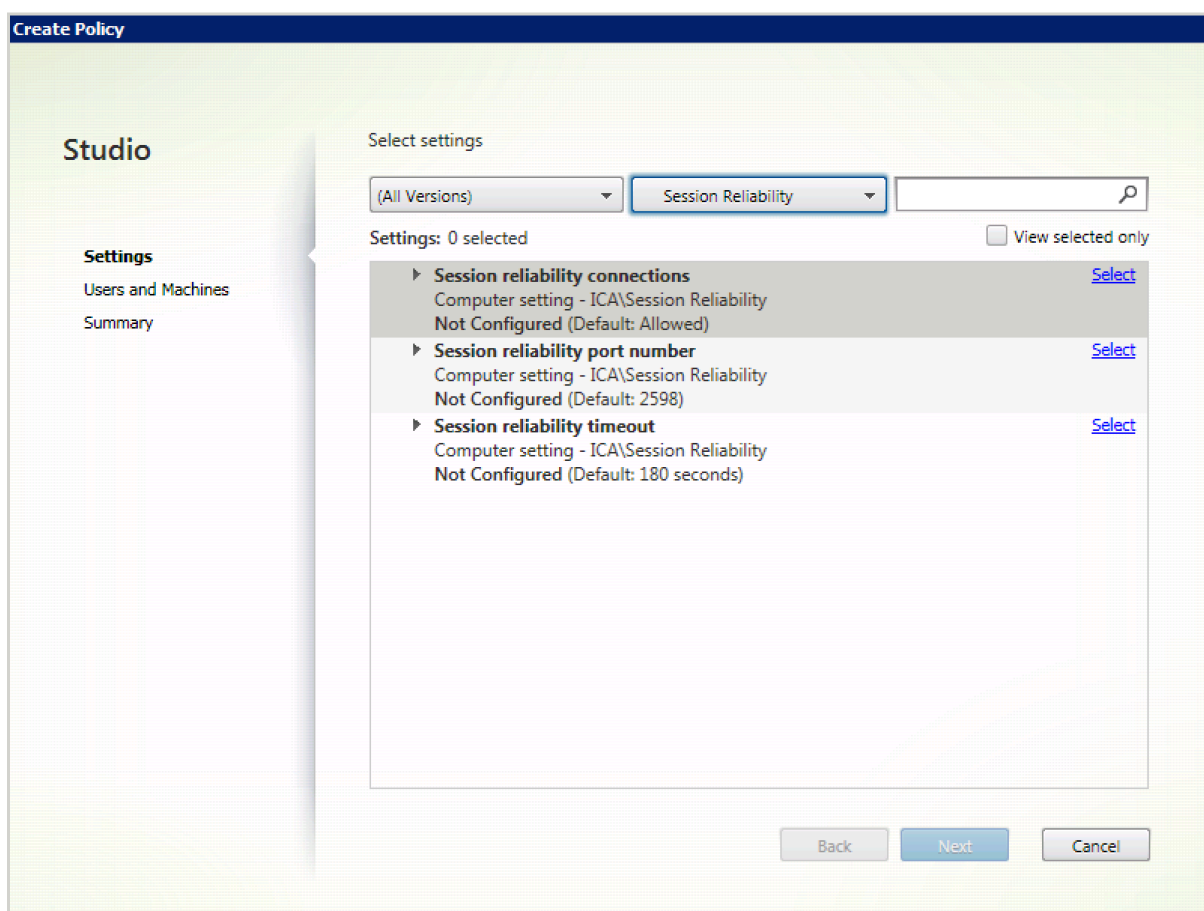
De forma predeterminada, la fiabilidad de sesión se habilita en el servidor. Para inhabilitar esta función, configure la directiva administrada por el servidor.

Configurar la fiabilidad de la sesión desde Citrix Studio

De forma predeterminada, la fiabilidad de la sesión está habilitada.

Para inhabilitar la fiabilidad de la sesión:

1. Abra Citrix Studio.
2. Abra la directiva **Conexiones de fiabilidad de la sesión**.
3. Establezca la directiva en **Prohibida**.



Configuración del tiempo de espera de la fiabilidad de la sesión

De manera predeterminada, el tiempo de espera de la fiabilidad de la sesión es de 180 segundos.

Nota:

La directiva tiempo de espera de fiabilidad de la sesión se puede configurar solo en XenApp y XenDesktop 7.11 y versiones posteriores.

Para modificar el tiempo de espera de la fiabilidad de la sesión:

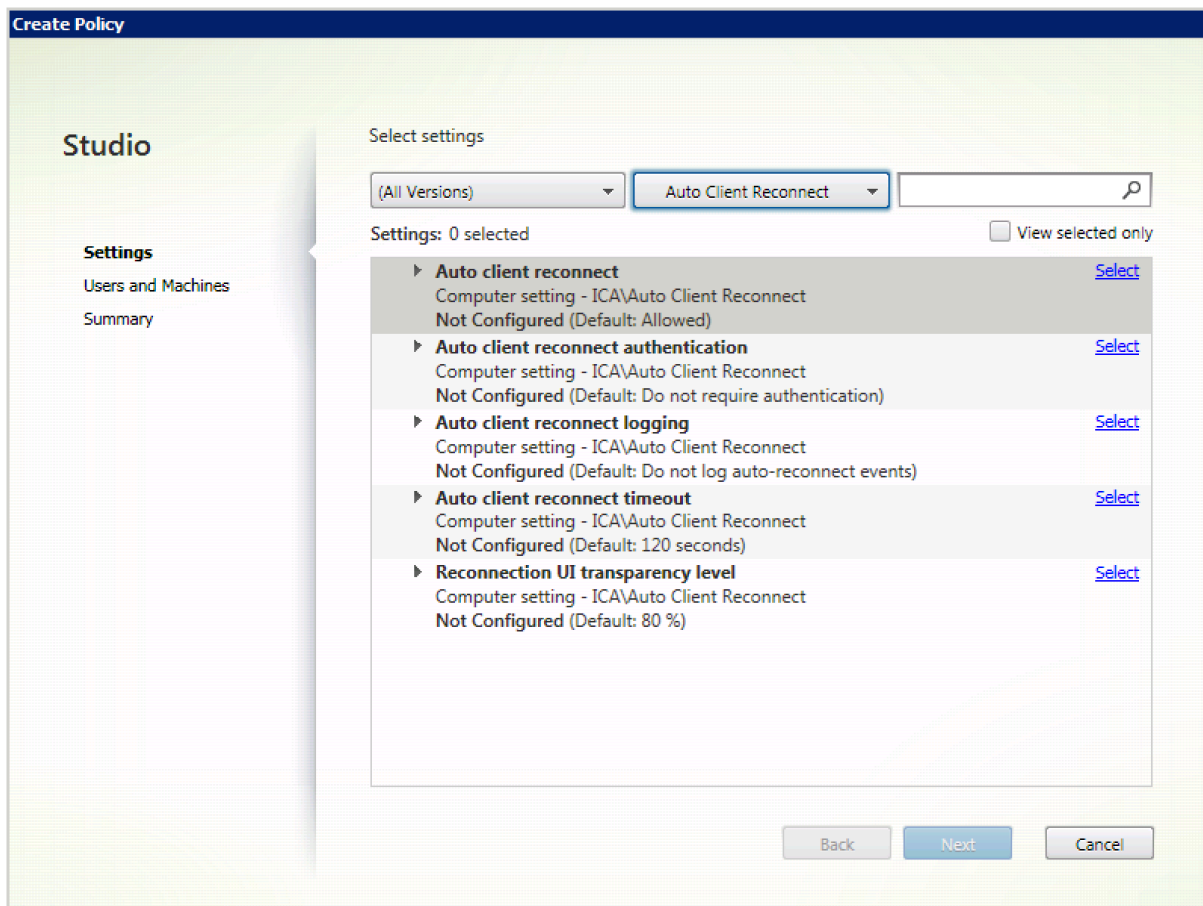
1. Abra Citrix Studio.
2. Abra la directiva **Tiempo de espera de fiabilidad de la sesión**.
3. Cambie el valor del tiempo de espera.
4. Haga clic en **Aceptar**.

Configurar la reconexión automática de clientes mediante Citrix Studio

De forma predeterminada, la reconexión automática de clientes está habilitada.

Para inhabilitar la reconexión automática de clientes

1. Abra Citrix Studio.
2. Abra la directiva **Reconexión automática de clientes**.
3. Establezca la directiva en **Prohibida**.



Configuración del tiempo de espera de la reconexión automática de clientes

De forma predeterminada, el tiempo de espera para la reconexión automática de clientes está establecido en 120 segundos.

Nota:

La directiva de tiempo de espera de reconexión automática de clientes solo se puede configurar con XenApp y XenDesktop 7.11 y versiones posteriores.

Para modificar el tiempo de espera de la reconexión automática de clientes:

1. Abra Citrix Studio.
2. Abra la directiva **Reconexión automática de clientes**.
3. Cambie el valor del tiempo de espera.
4. Haga clic en **Aceptar**.

Limitaciones:

En un VDA de Terminal Server, la aplicación Citrix Workspace para Mac usa 120 segundos como tiempo de espera independientemente de cómo se configuren los parámetros del usuario.

Configurar la transparencia de la interfaz de usuario de la reconexión

Durante los intentos de reconexión automática de clientes y de la función de fiabilidad de la sesión, la interfaz de usuario de la sesión sigue mostrándose. El nivel de transparencia de la interfaz de usuario se puede modificar mediante directiva en Studio.

De manera predeterminada, el nivel de transparencia de la interfaz de usuario es del 80%.

Para modificar el nivel de transparencia de la interfaz de usuario durante una reconexión:

1. Abra Citrix Studio.
2. Abra la directiva **Nivel de transparencia de la interfaz de usuario durante la reconexión**.
3. Cambie el valor.
4. Haga clic en **Aceptar**.

Interacción entre la fiabilidad de sesión y la reconexión automática de clientes

Existen problemas de movilidad asociados al cambio entre varios puntos de acceso, interrupciones de red y tiempos de espera de pantalla que están relacionados con la latencia. Complican los entornos al intentar mantener la integridad de los enlaces de las sesiones activas de Citrix Workspace para Mac. Las tecnologías mejoradas de fiabilidad de sesión y reconexión automática de Citrix resuelven este problema.

Esta función permite a los usuarios reconectarse a sesiones automáticamente después de recuperarse de interrupciones de la red. Estas funciones se habilitan mediante directivas en Citrix Studio y se pueden utilizar para mejorar la experiencia de usuario.

Nota:

Los valores de tiempo de espera de la reconexión automática del cliente y la fiabilidad de la sesión se pueden modificar en el archivo **default.ica** de StoreFront.

Reconexión automática de clientes

La reconexión automática de clientes se puede habilitar o inhabilitar mediante las directivas de Citrix Studio. De manera predeterminada, esta función está habilitada. Para obtener más información sobre cómo modificar esta directiva, consulte la sección sobre la reconexión automática de clientes más arriba en este artículo.

Utilice el archivo `default.ica` de StoreFront para modificar el tiempo de espera de conexión de Auto-ClientReconnect. De forma predeterminada, este tiempo de espera se establece en 120 segundos (o dos minutos).

Parámetro	Ejemplo	Valor predeterminado
TransportReconnectRetryMaxT!	TransportReconnectRetryMaxT!	120

Fiabilidad de la sesión

La fiabilidad de la sesión se puede habilitar o inhabilitar mediante las directivas de Citrix Studio. De manera predeterminada, esta función está habilitada.

Utilice el archivo **default.ica** de StoreFront para modificar el tiempo de espera de conexión de la fiabilidad de la sesión. De forma predeterminada, este tiempo de espera es de 180 segundos (3 minutos).

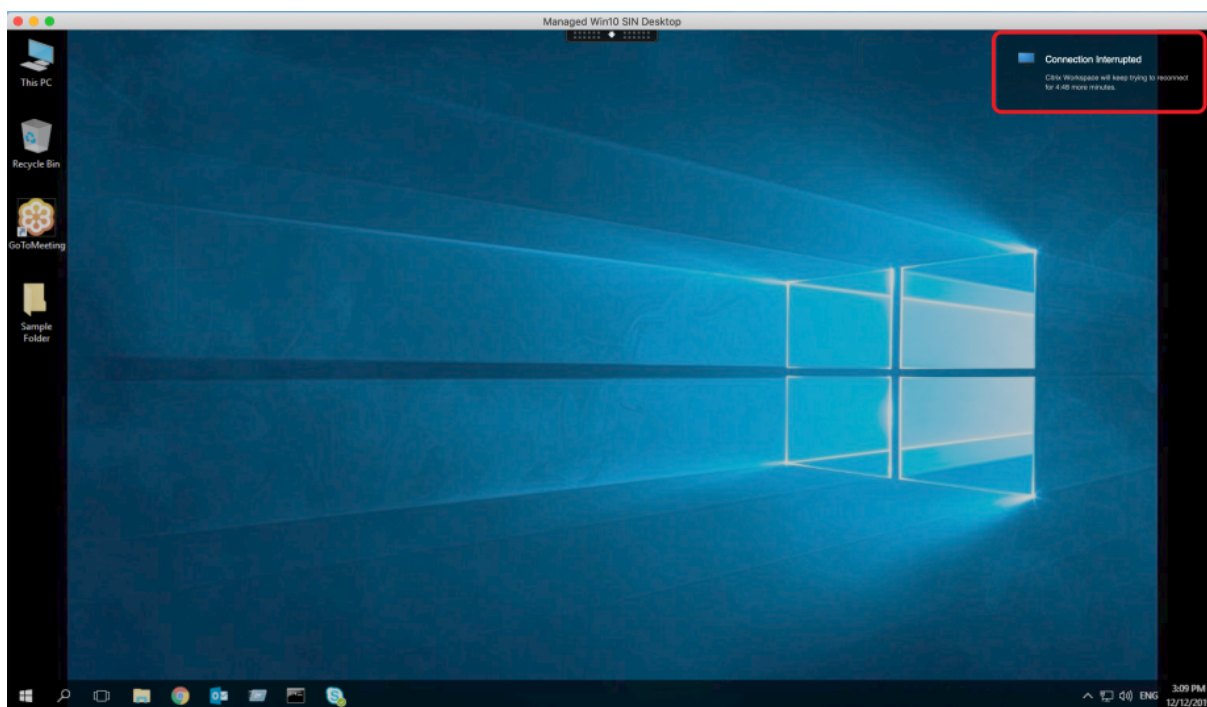
Parámetro	Ejemplo	Valor predeterminado
SessionReliabilityTTL	SessionReliabilityTTL=120	180

Cómo funcionan la reconexión automática de clientes y la fiabilidad de la sesión

Cuando la reconexión automática de clientes y la fiabilidad de la sesión están habilitadas en la aplicación Citrix Workspace para Mac, tenga en cuenta lo siguiente:

- La ventana de la sesión se oscurece mientras tiene lugar una reconexión. Aparece un temporizador que muestra el tiempo restante antes de volver a conectarse a la sesión. Cuando se supera el tiempo de espera, la sesión se desconecta.

De forma predeterminada, la notificación de cuenta atrás de reconexión comienza en 5 minutos. El valor de este temporizador representa los valores predeterminados combinados de cada temporizador (el de la reconexión automática del cliente y el de la fiabilidad de la sesión), que son 2 y 3 minutos, respectivamente. En la imagen siguiente se puede ver la notificación de la cuenta atrás, que aparece en la sección superior derecha de la interfaz de la sesión:

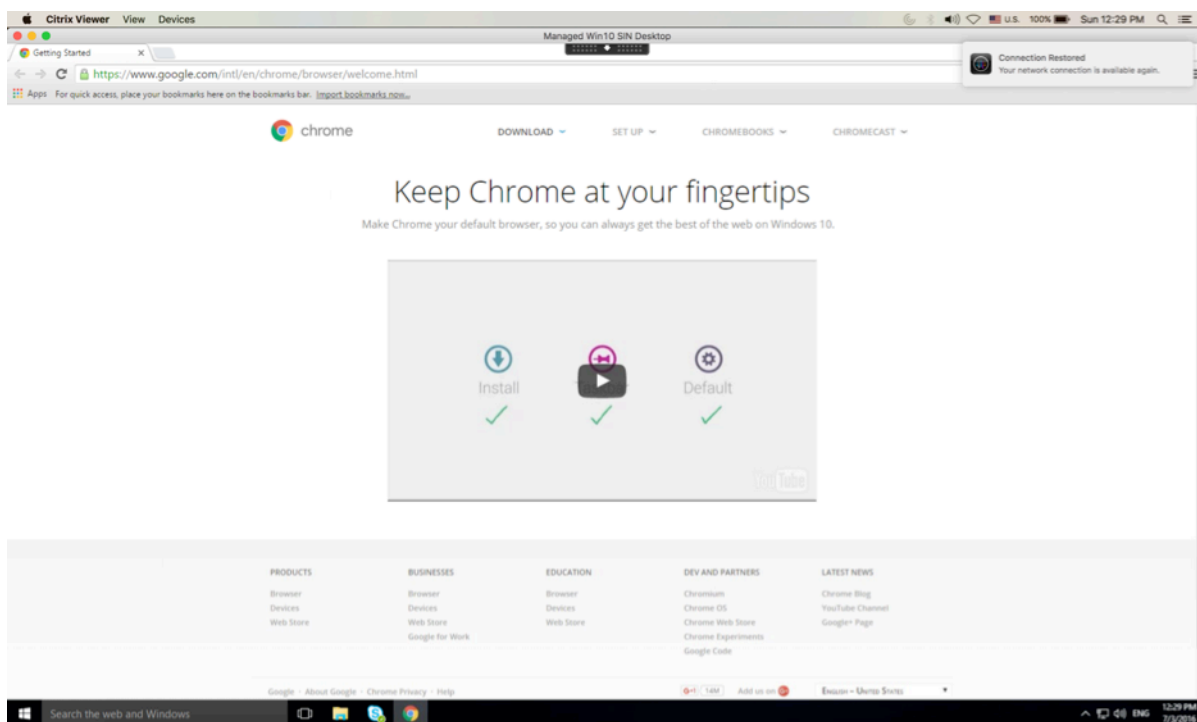


Sugerencia

Se puede modificar el brillo de la escala de grises utilizado para una sesión inactiva, mediante la interfaz de comandos. Por ejemplo: `defaults write com.citrix.receiver.nomas NetDisruptBrightness 80`. De forma predeterminada, este valor está establecido en 80. El valor máximo es 100 (esto indica una ventana transparente) y el valor mínimo es 0 (esto indica una pantalla en negro).

- Los usuarios ven una notificación cuando la sesión se reconecta correctamente (o cuando la sesión se desconecta). Esta notificación aparece en la sección superior derecha de la interfaz de la sesión:

Aplicación Citrix Workspace para Mac



- La ventana de una sesión que está bajo el control de las funciones de reconexión automática de clientes y fiabilidad de la sesión presenta un mensaje informativo donde se indica el estado de la conexión de la sesión. Haga clic en **Cancelar reconexión** para volver a una sesión activa.

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

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 Workspace para Mac 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 Workspace.

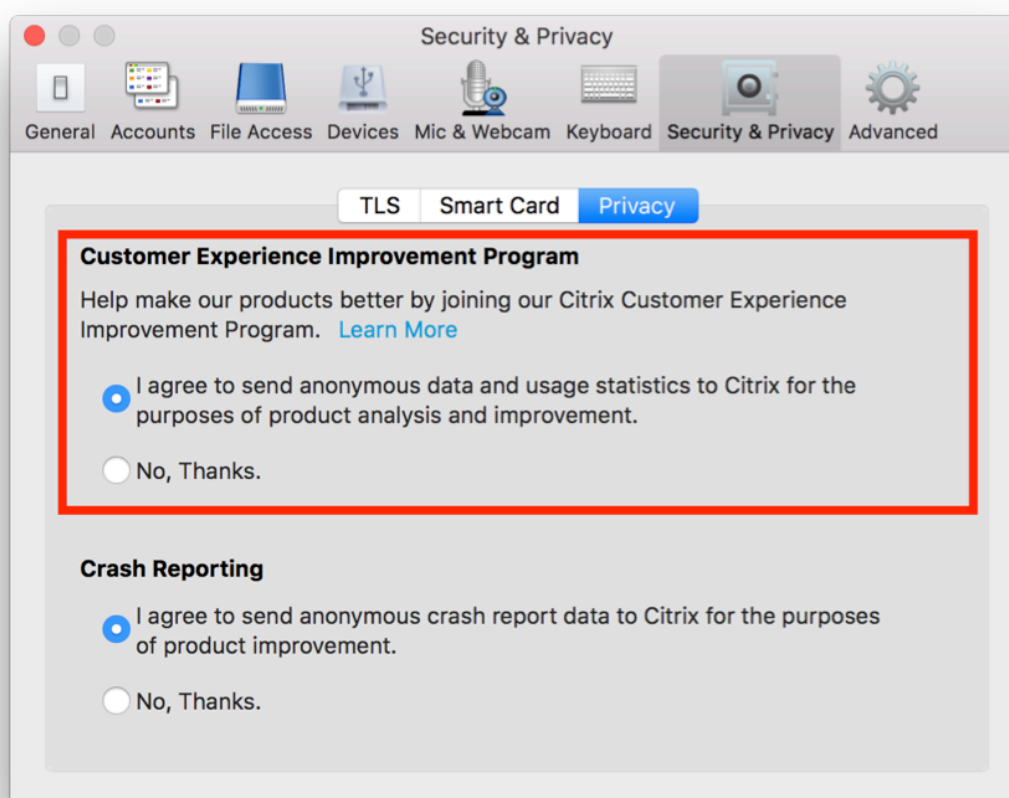
Información adicional

Citrix gestiona sus datos de acuerdo con las condiciones de su contrato con Citrix. Sus datos están protegidos, de acuerdo con el documento [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. Consulte [cómo gestiona Google los datos recopilados para Google Analytics](#).

Para inhabilitar el envío de datos de CEIP a Citrix y Google Analytics, siga estos pasos:

1. En la ventana **Preferencias**, seleccione **Seguridad y privacidad**.
2. Seleccione la ficha **Privacidad**.
3. Seleccione **No, gracias** para inhabilitar CEIP o dejar de participar en el programa.
4. Haga clic en **Aceptar**.



También puede inhabilitar el programa CEIP mediante este comando de la terminal:

```
defaults write com.citrix.receiver.nomas "CEIPEnabled"-bool NO
```

Los elementos de datos específicos que recopila Google Analytics son:

Versión del sistema operativo	Inicio de sesiones	Uso de la redirección de USB genérico
-------------------------------	--------------------	---------------------------------------

Entrega de aplicaciones

Cuando entregue aplicaciones con Citrix Virtual Apps and Desktops, tenga en cuenta las siguientes opciones para mejorar la experiencia de los usuarios que acceden a las aplicaciones:

Modo de acceso web

Sin necesidad de configuración, la aplicación Citrix Workspace para Mac ofrece el modo de acceso Web: acceso mediante un explorador web a las aplicaciones y escritorios. Los usuarios simplemente abren un explorador web para ir a un sitio de Workspace para Web y allí seleccionan y usan las aplicaciones que quieren. En el modo de acceso Web, no se colocan accesos directos de aplicaciones en la carpeta de Aplicaciones del dispositivo de usuario.

Modo de autoservicio

Agregue una cuenta de StoreFront a la aplicación Citrix Workspace para Mac o configure la aplicación Citrix Workspace para Mac para que apunte a un sitio de StoreFront. A continuación, puede configurar el modo de autoservicio, que permite a los usuarios suscribirse a las aplicaciones a través de la aplicación Citrix Workspace para Mac. Esta experiencia de usuario mejorada es similar al uso de un almacén de aplicaciones móviles. En el modo de autoservicio se pueden configurar parámetros de palabra clave para aplicaciones aprovisionadas automáticamente, destacadas y obligatorias. Cuando uno de sus usuarios selecciona una aplicación, se coloca un acceso directo para esa aplicación en la carpeta Aplicaciones del dispositivo del usuario.

Cuando acceden a un sitio de StoreFront 3.0, los usuarios ven una previsualización de la aplicación Citrix Workspace para Mac.

Al publicar aplicaciones en las comunidades de Citrix Virtual Apps, puede mejorar la experiencia de los usuarios que acceden a esas aplicaciones mediante almacenes de StoreFront. Asegúrese de incluir descripciones significativas para las aplicaciones publicadas. Las descripciones estarán visibles para los usuarios a través de la aplicación Citrix Workspace para Mac.

Configurar el modo de autoservicio

Como se mencionó anteriormente, puede agregar una cuenta de StoreFront a la aplicación Citrix Workspace para Mac o configurar la aplicación Citrix Workspace para Mac para que apunte a un sitio de StoreFront. Por lo tanto, puede configurar el modo de autoservicio, que permite a los usuarios suscribirse a las aplicaciones desde la interfaz de usuario de la aplicación Citrix Workspace para Mac. Esta experiencia de usuario mejorada es similar al uso de un almacén de aplicaciones móviles.

En el modo de autoservicio, se pueden configurar parámetros de palabra clave para aplicaciones aprovisionadas automáticamente, destacadas y obligatorias.

- Para suscribir automáticamente todos los usuarios de un almacén a una aplicación, agregue la cadena ****KEYWORDS:Auto**** a la descripción mientras publica la aplicación en Citrix Virtual Apps. Cuando los usuarios inicien sesión en el almacén, la aplicación se aprovisionará automáticamente, sin necesidad de que los usuarios tengan que suscribirse de forma manual a la aplicación.
- Si quiere anunciar aplicaciones o facilitar a los usuarios la búsqueda de las aplicaciones más utilizadas, indíquelas en la lista Destacadas de la aplicación Citrix Workspace para Mac. Para mostrar aplicaciones en la lista de aplicaciones destacadas de Mac, agregue la cadena ****KEYWORDS:Featured**** a la descripción de la aplicación.

Para obtener más información, consulte la documentación de [StoreFront](#).

Actualizaciones de Citrix Workspace

Configuración mediante la GUI

Un usuario puede anular la configuración de **Actualizaciones de Citrix Workspace** desde el diálogo **Preferencias avanzadas**. Se trata de una configuración específica de cada usuario y los parámetros se aplican solamente al usuario actual.

1. Vaya al cuadro de diálogo **Preferencias** en la aplicación Citrix Workspace para Mac.
2. En el panel **Avanzado**, haga clic en **Actualizaciones**. Aparecerá el cuadro de diálogo Actualizaciones de Citrix Workspace.
3. Seleccione una de estas opciones:
 - Sí, notificarme
 - No, no notificarme
 - Usar parámetros especificados por el administrador
4. Cierre el cuadro de diálogo para guardar los cambios.

Configurar Actualizaciones de Citrix Workspace mediante StoreFront

Los administradores pueden configurar las Actualizaciones de Citrix Workspace con StoreFront. La aplicación Citrix Workspace para Mac solo usa esta configuración para los usuarios que han seleccionado “Usar parámetros especificados por el administrador”. Para configurarla manualmente, siga estos pasos.

1. Use un editor de texto para abrir el archivo web.config. La ubicación predeterminada es `C:\inetpub\wwwroot\Citrix\Roaming\web.config`
2. Localice el elemento de la cuenta de usuario en el archivo (Store es el nombre de cuenta de la implementación)

Por ejemplo: `<account id=... name=”Store”>`

Antes de la etiqueta `</account>`, vaya a las propiedades de esa cuenta de usuario:

`<properties>`

`<clear />`

`</properties>`

3. Agregue la etiqueta de actualización automática después de `<clear />`.

auto-update-Check

auto-update-Check determina que la aplicación Citrix Workspace para Mac puede detectar si hay actualizaciones disponibles.

Valores válidos:

- Auto: Se usa para recibir notificaciones cuando hay actualizaciones disponibles.
- Manual: Se usa para no recibir notificaciones cuando hay actualizaciones disponibles. Los usuarios deben buscar manualmente las actualizaciones. Para ello, deberán seleccionar **Comprobar actualizaciones**.
- Disabled: Se usa para inhabilitar las Actualizaciones de Citrix Workspace.

auto-update-DeferUpdate-Count

Determina la cantidad de veces que el usuario recibe notificaciones para actualizar la versión de la aplicación Citrix Workspace para Mac antes de obligarlo a actualizarla a la versión más reciente. El valor predeterminado es 7.

Valores válidos:

- -1: El usuario recibe un recordatorio más tarde cuando hay una actualización disponible.
- 0: Se obliga al usuario a que actualice a la versión más reciente de la aplicación Citrix Workspace para Mac cuando la actualización esté disponible.

- Número entero positivo: El usuario recibe esta cantidad de recordatorios antes de que se fuerce la actualización. Citrix recomienda no establecer este valor a más de 7.

auto-update-Rollout-Priority

Determina lo rápido que un dispositivo detecta que hay una actualización disponible.

Valores válidos:

- Auto: El sistema Actualizaciones de Citrix Workspace decide cuándo distribuyen a los usuarios las actualizaciones disponibles.
- Fast: Las actualizaciones disponibles se distribuyen a los usuarios con prioridad alta de la manera que lo determine la aplicación Citrix Workspace para Mac.
- Medium: Las actualizaciones disponibles se distribuyen a los usuarios con prioridad media de la manera que lo determine aplicación Citrix Workspace para Mac.
- Slow: Las actualizaciones disponibles se distribuyen a los usuarios con prioridad baja de la manera que lo determine aplicación Citrix Workspace para Mac.

Sincronización de la distribución de teclado

La sincronización de la distribución del teclado permite a los usuarios cambiar entre distintas distribuciones de teclado preferidas en el dispositivo cliente cuando utilice un VDA de Linux o de Windows. Esta función está inhabilitada de forma predeterminada.

Para habilitar la sincronización de la distribución de teclado, vaya a **Preferencias > Teclado** y seleccione “Usar la distribución de teclado local, en lugar de la distribución de teclado del servidor remoto”.

Nota:

1. El uso de la opción de distribución de teclado local activa el IME (Input Method Editor) del cliente. Los usuarios que trabajan en japonés, chino o coreano pueden utilizar el editor IME del servidor. Para ello, deben desmarcar la opción de distribución de teclado local en **Preferencias > Teclado**. La sesión recurrirá a la distribución de teclado que suministre el servidor remoto cuando se conecten a la sesión siguiente.
2. La función se puede utilizar en la sesión solamente cuando la opción está activada en el cliente y la función correspondiente está habilitada en el VDA. Se agrega un elemento de menú, **Usar la distribución de teclado del cliente**, en **Dispositivos > Teclado > Internacional**, para mostrar el estado habilitado.

Limitaciones

- Las distribuciones de teclado que figuran en **Distribuciones de teclado compatibles en Mac** funcionan al usar esta función. Cuando se cambia la distribución de teclado del cliente a una

distribución que no es compatible, es posible que se sincronice la distribución en el VDA, pero no se puede confirmar la funcionalidad.

- Las aplicaciones remotas que se ejecutan con privilegios elevados no se pueden sincronizar con la distribución del teclado del cliente. Para solucionar este problema, cambie manualmente la distribución del teclado en el VDA o inhabilite el control de cuentas de usuario (UAC).
- Cuando un usuario trabaja en una sesión RDP, no es posible cambiar la distribución del teclado con los accesos directos **Alt + Shift** cuando RDP se implementa como una aplicación. Como solución temporal, los usuarios pueden usar la barra de idioma de la sesión RDP para cambiar la distribución del teclado.

Compatibilidad de la distribución del teclado con Windows VDA

Supported keyboard layouts on Mac	
Language on Mac	Input source on Mac
English	US.
	U.S. International - PC
	Dvorak
	Dvorak - Left
	Dvorak - Right
	British
	British - PC
	Canadian English
	Australian
	Irish
French	French
	French - Numerical
	Canadian French - CSA
	Swiss French
	French - PC
German	German
	Austrian
	Swiss German
Spanish	Spanish
	Spanish - ISO
Bulgarian	Bulgarian
Swedish	Swedish
Czech	Czech
Danish	Danish
Finnish	Finnish
Hungarian	Hungarian
Italian	Italian
Greek	Greek
	Greek - PC
Dutch	Belgian
	Dutch
Romanian	Romanian - Standard
Russian	Russian - PC
Croatian	Croatian - PC
Slovak	Slovak
	Slovak - QWERTY
Turkish	Turkish
	Turkish - QWERTY PC
Portuguese	Brazilian
	Brazilian - ABNT2
	Portuguese
Ukrainian	Ukrainian - PC
Belarusian	Belarusian
Slovenian	Slovenian
Estonian	Estonian
Latvian	Latvian
Polish	Polish Pro
Icelandic	Icelandic
Norwegian	Norwegian
Japanese	Hiragana
	Katakana
	Romaji
Korean	2-Set Korean
	3-Set Korean
Chinese, Simplified	
Chinese, Traditional	

Compatibilidad de la distribución del teclado con Linux VDA

Language in MAC	Input Source in MAC
English	US.
	U.S. International - PC
	Dvorak
	Dvorak - Left
	Dvorak - Reft
	British
	British - PC
	Candian English
	Australian
	Irish
French	French
	French - Numerical
	Canadian French - CSA
	Swiss French
	French - PC
German	German
	Austrian
	Swiss German
Spanish	Spanish
	Spanish - ISO
Swedish	Swedish
Czech	Czech
Danish	Danish
Finnish	Finnish
Hungarian	Hungarian
Italian	Italian
Greek	Greek
Dutch	Belgian
	Dutch
Russian	Russian - PC
Croatian	Croatian - PC
Slovak	Slovak
	Slovak - QWERTY
Turkish	Turkish
	Turkish - QWERTY PC
Portuguese	Brazilian
	Brazilian - ABNT2
	Portuguese
Ukrainian	Ukrainian - PC
Belarusian	Belarusian
Slovenian	Slovenian
Estonian	Estonian
Polish	Polish Pro
Icelandic	Icelandic
Norwegian	Norwegian
Japanese	Hiragana
	Katakana
	Romaji
Korean	2-Set Korean
	3-Set Korean
Chinese, Simplified	Pinyin -Simplified
Chinese, Traditional	Pinyin - Traditional

El cliente mejorado depende de la función de sincronización de la distribución del teclado. De forma predeterminada, la función mejorada está habilitada cuando se activa la funcionalidad de sincronización de distribución de teclado. Para controlar esta función de manera independiente, abra el archivo **Config** en la carpeta `~/Library/Application Support/Citrix Receiver/`, busque el parámetro “**EnableIMEEnhancement**” y active o desactive la función, mediante “true” o “false,” respectivamente.

Nota:

El cambio de este parámetro tiene efecto después de reiniciar la sesión.

Barra de idioma

Puede optar por mostrar u ocultar la barra remota de idioma en una sesión de aplicación mediante la GUI. La barra de idioma muestra el idioma de entrada preferido en una sesión. En versiones anteriores, solo podía cambiar esta configuración mediante las claves de Registro en el VDA. A partir de la versión 1808 de Citrix Workspace para Mac, puede cambiar la configuración mediante el cuadro de diálogo **Preferencias**. La barra de idioma aparece en una sesión de forma predeterminada.

Nota:

Esta función está disponible en sesiones con VDA 7.17 y versiones posteriores.

Definir si mostrar u ocultar la barra de idioma remota

1. Abrir Preferencias.
2. Haga clic en Teclado.
3. Haga clic en Mostrar la barra de idiomas remota para las aplicaciones publicadas.

Nota:

Los cambios de configuración surten efecto de inmediato. Puede cambiar la configuración en una sesión activa. La barra de idioma remota no aparece en una sesión si solo hay un idioma de entrada.

Citrix Casting

Citrix Casting se utiliza para proyectar la pantalla de su Mac en dispositivos cercanos de Citrix Ready Workspace Hub. La aplicación Citrix Workspace para Mac admite Citrix Casting para duplicar la pantalla de su Mac en monitores conectados al Workspace Hub.

Para obtener más información, consulte la documentación de [Citrix Ready Workspace Hub](#).

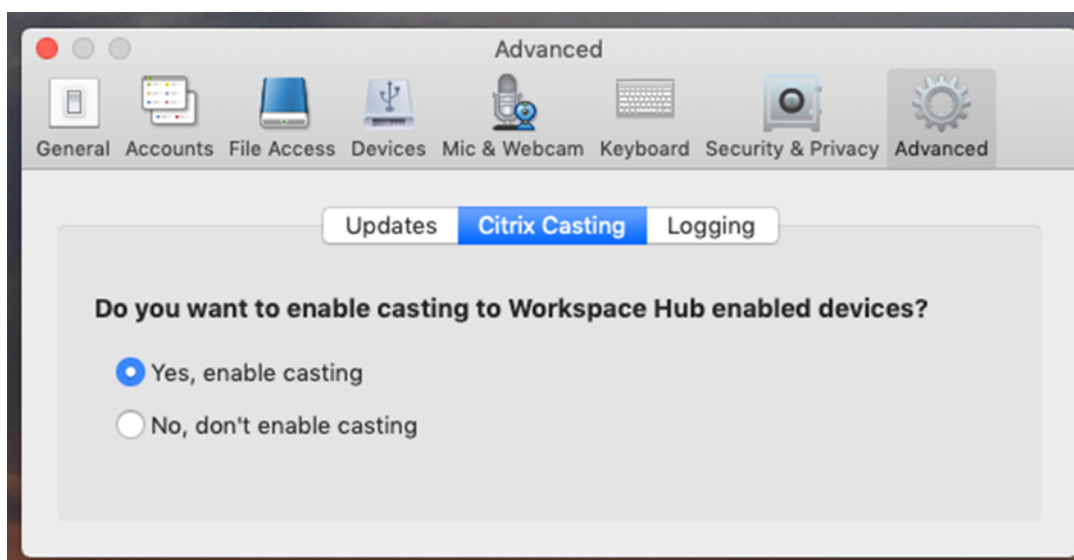
Requisitos previos

- Aplicación Citrix Workspace 1812 para Mac o una versión posterior.
- Bluetooth está habilitado en el dispositivo para detectar hubs.
- Tanto Citrix Ready Workspace Hub como la aplicación Citrix Workspace deben estar en la misma red.
- Compruebe que el puerto 55555 no está bloqueado entre el dispositivo que ejecuta la aplicación Citrix Workspace y Citrix Ready Workspace Hub.
- El puerto 55556 es el puerto predeterminado para las conexiones SSL entre los dispositivos móviles y Citrix Ready Workspace Hub. Puede configurar otro puerto SSL en la página de parámetros de Raspberry Pi. Si el puerto SSL está bloqueado, los usuarios no pueden establecer conexiones SSL con Workspace Hub.
- Para Citrix Casting, el puerto 1494 no debe estar bloqueado.

Habilitar Citrix Casting

Citrix Casting está inhabilitado de forma predeterminada. Para habilitar Citrix Casting mediante la aplicación Citrix Workspace para Mac:

1. Vaya a **Preferencias**.
2. Seleccione **Preferencias avanzadas** en el panel y luego elija **Citrix Casting**.
3. Seleccione **Sí, habilitar proyección**.



Aparecerá una notificación cuando se inicia Citrix Casting y aparece un icono de Citrix Casting en la barra de menús.

Nota:

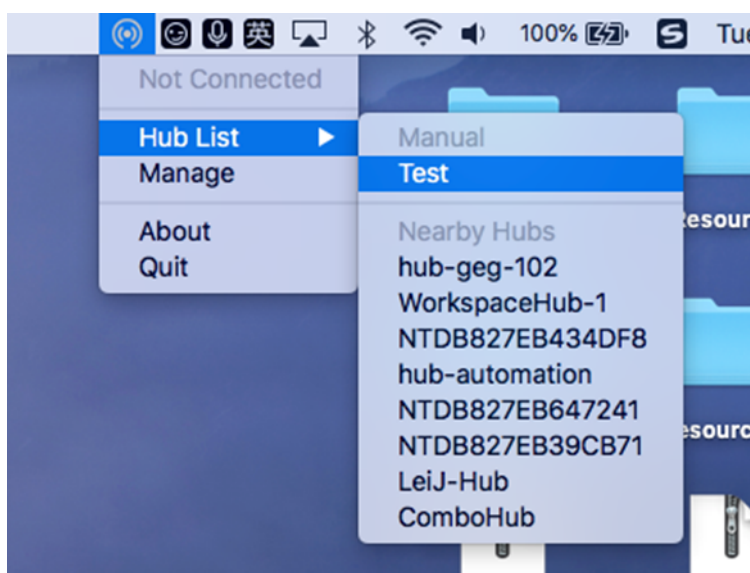
Una vez habilitado, Citrix Casting se inicia automáticamente con la aplicación Citrix Workspace

para Mac hasta que lo inhabilite seleccionando **No, no habilitar proyección** en **Preferencias > Avanzadas > Citrix Casting**.

Detectar dispositivos Workspace Hub automáticamente

Para conectarse automáticamente a los Workspace Hubs:

1. En el Mac, inicie sesión en la aplicación Citrix Workspace y compruebe que el Bluetooth esté activado. El Bluetooth se utiliza para detectar los Workspace Hubs cercanos.
2. Seleccione el icono de **Citrix Casting** de la barra de menú. Todas las funciones de Citrix Casting operan a través de este menú.
3. En el submenú **Lista de hubs** se muestran todos los Workspace Hubs cercanos en la misma red. Los hubs se muestran en orden descendente según su proximidad a tu Mac y muestran los nombres configurados de Workspace Hub. Todos los hubs detectados automáticamente se muestran en **Hubs cercanos**.
4. Para elegir el hub al que quiere conectarse, seleccione su nombre.



Para cancelar la selección de un Workspace Hub durante la conexión, seleccione **Cancelar**. También puede utilizar **Cancelar** si la conexión de red es de poca calidad y la conexión tarda más de lo habitual.

Nota:

En ocasiones, es posible que el hub elegido no aparezca en el menú. Vuelva a comprobar el menú **Lista de hub** después de unos instantes o agregue el hub manualmente. Citrix Casting recibe periódicamente las difusiones de Workspace Hub.

Detectar dispositivos Workspace Hub de forma manual

Si no puede encontrar el dispositivo Citrix Ready Workspace Hub en el menú **Lista de hubs**, agregue la dirección IP del dispositivo Workspace Hub para acceder a él manualmente. Para agregar un Workspace Hub:

1. En el Mac, inicie sesión en la aplicación Citrix Workspace y compruebe que el Bluetooth esté activado. El Bluetooth se utiliza para detectar los Workspace Hubs cercanos.
2. Seleccione el icono de **Citrix Casting** de la barra de menú.
3. Seleccione **Administrar** en el menú. Aparecerá la ventana **Administrar hubs**.
4. Haga clic en **Agregar** para introducir la dirección IP del hub.
5. Tras agregar correctamente el dispositivo, la columna **Nombre del hub** muestra el nombre descriptivo del hub. Utilice este nombre para identificar el hub en la sección **Manual** del submenú **Lista de hubs**.

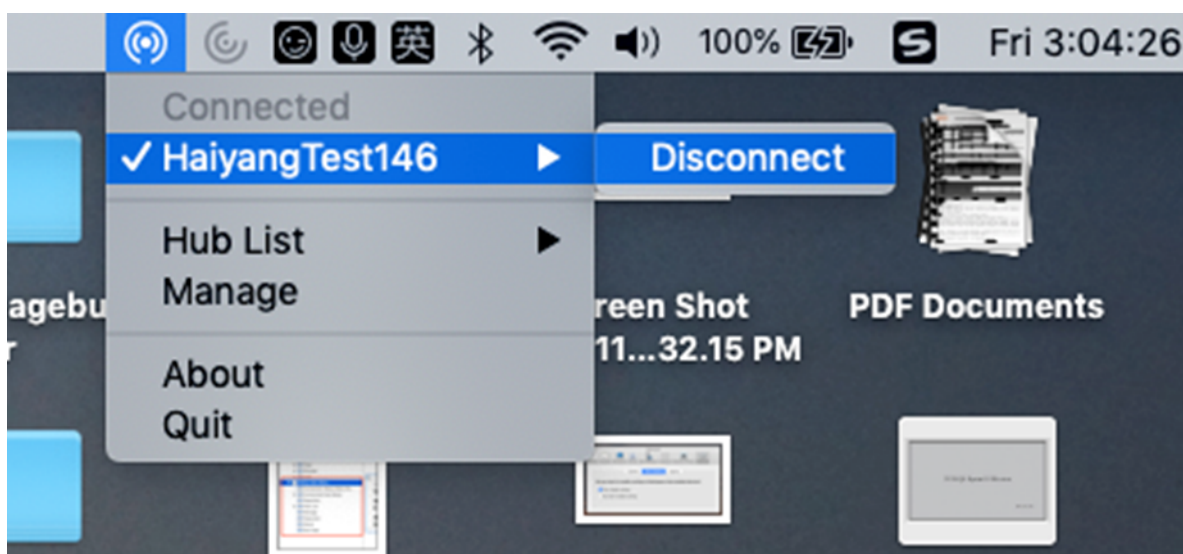
Nota:

Actualmente, solo se admite el modo **Duplicar**. **Duplicar** es la única opción disponible en la columna **Modo de pantalla**.

Desconectar el dispositivo Workspace Hub

Puede desconectar la sesión actual y salir de Citrix Ready Workspace Hub de forma automática o manual.

- Para desconectar automáticamente la sesión de proyección de pantalla, cierre el portátil.
- Para desconectar la sesión de proyección de pantalla manualmente:
 1. Seleccione el icono de **Citrix Casting**.
 2. En la lista de hubs, seleccione el nombre del Workspace Hub. Aparecerá la opción **Desconectar** a la derecha.
 3. Seleccione **Desconectar** para salir del hub.



Problemas conocidos

- Hay pequeños problemas de latencia al visualizar la pantalla duplicada. En casos de mala conexión, la latencia puede ser aún más larga.
- Cuando SSL está habilitado en un hub de Citrix Ready Workspace Hub y el certificado del concentrador no es de confianza, aparece una ventana de alerta. Para solucionar el problema, agregue el certificado a su lista de certificados de confianza con la herramienta Llavero.

Entrada de micrófono en el cliente

La aplicación Citrix Workspace para Mac admite varias entradas de micrófono en el cliente. Los micrófonos instalados localmente se pueden usar para:

- Eventos en tiempo real, como llamadas desde sistemas de telefonía integrada en el equipo y conferencias web.
- Aplicaciones de grabación en el servidor, como programas de dictado.
- Grabaciones de vídeo y sonido.

La aplicación Citrix Workspace para Mac admite el dictado digital.

Para utilizar micrófonos conectados a su dispositivo, seleccione una de estas opciones en los parámetros de **Micrófono y cámara web**, en **Aplicación Citrix Workspace para Mac > Preferencias**:

- Usar mi micrófono y cámara web
- No usar mi micrófono y cámara web
- Preguntar siempre

Si marca **Preguntar siempre**, aparecerá un cuadro de diálogo cada vez que se conecte, donde se le preguntará si quiere utilizar el micrófono en esa sesión.

Teclas especiales de Windows

La aplicación Citrix Workspace para Mac ofrece diversas opciones y formas fáciles de sustituir teclas especiales, como las teclas de función de las aplicaciones de Windows, por teclas de Mac. Para configurar las opciones que quiere usar, utilice la ficha **Teclado** de la siguiente manera:

- “Enviar el carácter Control mediante” le permite seleccionar si se quieren enviar combinaciones de teclas Comando-tecla de carácter como combinaciones Ctrl+tecla de carácter dentro de una sesión. Si selecciona “Comando o Control” en el menú emergente, puede enviar combinaciones conocidas de teclas Comando-tecla de carácter o Ctrl-tecla de carácter en Mac a los PC como combinaciones Ctrl+tecla de carácter. Si se selecciona Control, se deben usar combinaciones de teclas Ctrl+tecla de carácter.
- “Enviar el carácter Alt mediante” permite seleccionar la forma de replicar la tecla Alt dentro de una sesión. Si selecciona Comando-Opción, puede enviar combinaciones de Comando-Opción y tecla como combinaciones de tecla Alt+ dentro de una sesión. De forma alternativa, si se selecciona Comando, es posible usar la tecla Comando como la tecla Alt.
- “Enviar tecla con el logotipo de Windows mediante Comando (a la derecha).” Permite enviar la tecla del logotipo de Windows a las aplicaciones y los escritorios remotos al presionar la tecla Comando ubicada a la derecha del teclado. Si esta opción se encuentra inhabilitada, la tecla Comando de la derecha presenta el mismo comportamiento que la tecla Comando de la izquierda según la configuración de los dos parámetros anteriores en el panel de preferencias. Sin embargo, aún puede enviar la tecla del logotipo de Windows mediante el menú Teclado. Para ello, seleccione **Teclado > Enviar acceso directo de Windows > Inicio**.
- “Enviar teclas especiales sin cambios” le permite inhabilitar la conversión de teclas especiales. Por ejemplo, la combinación Opción-1 (en el teclado numérico) es equivalente a la tecla especial F1. Es posible modificar este comportamiento y establecer que esta tecla especial represente 1 (el número uno en el teclado) en la sesión. Para eso, marque la casilla “Enviar teclas especiales sin cambios”. De forma predeterminada, esta casilla de verificación no está marcada, por lo que Opción-1 se envía a la sesión como F1.

El menú **Teclado** permite enviar teclas de función y otras teclas especiales a una sesión.

Si el teclado incluye un teclado numérico, también es posible usar las siguientes pulsaciones de teclas:

Acción o tecla de PC	Opciones de Mac
INSERTAR	0 (el número cero) en el teclado numérico. La tecla Bloq num debe estar desactivada; es posible activarla y desactivarla mediante la tecla Borrar ; Opción-Ayuda

Acción o tecla de PC	Opciones de Mac
SUPRIMIR	Punto decimal en el teclado numérico. La tecla Bloq num debe estar desactivada; es posible activarla y desactivarla mediante la tecla Borrar ; Borrar
De F1 a F9	Opción-1 a -9 (los números del uno al nueve) en el teclado numérico
F10	Opción-0 (el número cero) en el teclado numérico
F11	Opción-signo menos en el teclado numérico
F12	Opción-signo más en el teclado numérico

Accesos directos y combinaciones de teclas de Windows

Las sesiones remotas reconocen la mayoría de las combinaciones de teclado Mac para la entrada de texto, como Opción-G para introducir el símbolo de copyright ©. No obstante, algunas pulsaciones de teclado que se realizan durante una sesión no se muestran en la aplicación o el escritorio remoto. El sistema operativo Mac las interpreta. Esto puede provocar que las teclas generen respuestas de Mac.

Es posible que necesite usar ciertas teclas de Windows, como la tecla Insertar, que no existen en muchos teclados de Mac. De forma similar, algunos accesos directos de teclado de Windows 8 muestran botones de acceso y comandos de aplicación, y permiten acoplar y cambiar aplicaciones. Los teclados Mac no imitan estos accesos directos. Sin embargo, estos pueden enviarse al escritorio remoto o a la aplicación desde el menú **Teclado**.

Los teclados y la configuración de las teclas pueden diferir considerablemente de un equipo a otro. Por ese motivo, la aplicación Citrix Workspace para Mac ofrece diversas opciones para garantizar que las pulsaciones de teclado puedan enviarse correctamente a las aplicaciones y los escritorios alojados. Estas pulsaciones de teclas se indican en la tabla. Se describe el comportamiento predeterminado. Si se ajustan los valores predeterminados (mediante las preferencias de la aplicación Citrix Workspace u otro programa), es posible que se reenvíen combinaciones de teclas diferentes y se observen otros comportamientos en el acceso con Remote PC.

Importante

Ciertas combinaciones de teclas detalladas en la tabla no se encuentran disponibles cuando se utilizan teclados Mac más nuevos. En la mayoría de estos casos, las entradas de teclado se pueden enviar a la sesión mediante el menú Teclado.

Convenciones utilizadas en la tabla:

- Las teclas de letras figuran en mayúscula, pero no implican que sea necesario presionar simultáneamente la tecla Mayús.
- Los guiones entre las pulsaciones de teclado indican que las teclas se deben presionar juntas (por ejemplo, Control-C).
- Las teclas de caracteres crean entradas de texto e incluyen todas las letras, números y signos de puntuación. Las teclas especiales no crean entradas de texto por sí mismas, sino que actúan como modificadores o controladores. Las teclas especiales incluyen Control, Alt, Mayús, Comando, Opción, teclas de flecha y teclas de función.
- Las instrucciones para los menús corresponden a los menús de la sesión.
- Según la configuración del dispositivo de usuario, es posible que algunas combinaciones de teclas no funcionen de la forma esperada y se enumeren combinaciones alternativas.
- Fn se refiere a la tecla Fn (Función) de los teclados de Mac. La tecla de función hace referencia desde F1 a F12 en teclados de PC o Mac.

Tecla o combinación de teclas de Windows	Equivalentes de Mac
Alt+tecla de carácter	Comando-Opción-tecla de carácter (por ejemplo, utilice Comando-Opción-C para enviar Alt-C)
Alt+tecla especial	Opción-tecla especial (por ejemplo, Opción-Tab); Comando-Opción-tecla especial (por ejemplo, Comando-Opción-Tab)
Ctrl+tecla de carácter	Comando-tecla de carácter (por ejemplo, Comando-C); Control-tecla de carácter (por ejemplo, Control-C)
Ctrl+tecla especial	Control-tecla especial (por ejemplo, Control-F4); Comando-tecla especial (por ejemplo, Comando-F4)
Ctrl/Alt/Mayús/Logotipo de Windows+tecla de función	**Seleccione Teclado > Enviar tecla de función** > Control/Alt/Mayús/Comando-tecla de función
Ctrl+Alt	Control-Opción-Comando
Ctrl+Alt+Suprimir	Control-Opción-Fn-Comando-Suprimir; seleccione Teclado > Enviar Ctrl-Alt-Supr
Suprimir	Suprimir; seleccione Teclado > Enviar clave > Suprimir; Fn-Retroceso (Fn-Suprimir en algunos teclados para Estados Unidos)
Fin	Fin; Fn-Flecha derecha

Tecla o combinación de teclas de Windows	Equivalentes de Mac
Esc	Escapar; seleccione Teclado > Enviar tecla > Escapar
De F1 a F12	De F1 a F12; seleccione Teclado > Enviar tecla de función > De F1 a F12
Inicio	Página; Fn-Tecla izquierda
Insertar	Seleccione Teclado > Enviar tecla > Insertar
Bloq num	Borrar
Av Pág	Av Pág; Fn-Tecla abajo
Re Pág	Re Pág; Fn-Tecla arriba
Barra espaciadora	Seleccione Teclado > Enviar tecla > Espacio
Tabulador	Seleccione Teclado > Enviar tecla > Tab
Logotipo de Windows	Tecla de comando a la derecha (una preferencia de teclado habilitada de forma predeterminada); seleccione Teclado > Enviar acceso directo de Windows > Inicio
Combinación de teclas para mostrar botones de acceso	Seleccione Teclado > Enviar acceso directo de Windows > Botones de acceso
Combinación de teclas para mostrar comandos de aplicación	Seleccione Teclado > Enviar acceso directo de Windows > Comandos de aplicación
Combinación de teclas para acoplar aplicaciones	Seleccione Teclado > Enviar acceso directo de Windows > Acoplar
Combinación de teclas para cambiar aplicaciones	Seleccione Teclado > Enviar acceso directo de Windows > Cambiar aplicaciones

Uso de editores IME y distribuciones de teclado internacionales

La aplicación Citrix Workspace para Mac permite utilizar un editor de métodos de entrada (IME) en el dispositivo de usuario o en el servidor.

Cuando el editor IME en el cliente está habilitado, los usuarios pueden introducir texto en el punto de inserción en lugar de en una ventana aparte.

La aplicación Citrix Workspace para Mac también permite que los usuarios especifiquen la distribución del teclado que quieren utilizar.

Para habilitar el editor IME en el cliente

1. En la barra de menús Citrix Viewer, elija **Teclado > Internacional > Usar IME del cliente**.
2. Asegúrese de que el editor IME en el servidor esté establecido en el modo alfanumérico o de entrada directa.
3. Utilice el IME de Mac para introducir texto.

Para indicar de forma explícita el punto de partida al introducir texto

- En la barra de menús Citrix Viewer, elija **Teclado > Internacional > Usar marca de composición**.

Para usar el editor IME en el servidor

- Asegúrese de que el editor IME en el cliente esté establecido en el modo alfanumérico.

Teclas de modo de entrada asignadas para el editor IME en el servidor

La aplicación Citrix Workspace para Mac ofrece asignaciones de teclado para las teclas de modo de entrada para el editor IME de Windows en el servidor que no se encuentran disponibles en los teclados Mac. En los teclados Mac, la tecla **Opción** se asigna a estas teclas de modo de entrada para el editor IME en el servidor, según la configuración regional en el servidor:

Configuración regional del sistema en el servidor	Tecla de modo de entrada para el editor IME en el servidor
Japonés	Tecla Kanji (Alt + Hankaku/Zenkaku en un teclado japonés)
Coreano	Tecla Alt derecha (alternancia hangul/inglés en un teclado coreano)

Para utilizar distribuciones internacionales de teclado

- Asegúrese de que las distribuciones de teclado en el cliente y en el servidor tengan la misma configuración regional que el idioma de entrada predeterminado en el servidor.

Varios monitores

Los usuarios pueden configurar la aplicación Citrix Workspace para Mac para que funcione en modo de pantalla completa abarcando varios monitores.

1. Abra Citrix Viewer.

2. En la barra de herramientas de Citrix Viewer, seleccione una de estas opciones según sus requisitos:
 - **Entrar en Pantalla completa:** Pantalla completa solamente en el monitor principal.
 - **Usar todas las pantallas en pantalla completa:** Pantalla completa en todos los monitores conectados.
3. Arrastre la pantalla Citrix Virtual Desktops entre los monitores.

La pantalla se extenderá a todos los monitores.

Limitaciones conocidas

- El modo de pantalla completa solo se admite en uno o en todos los monitores, los cuales pueden configurarse mediante una opción de menú.
- Citrix recomienda utilizar un máximo de 2 monitores. El uso de más de 2 monitores puede degradar el rendimiento de la sesión o causar problemas de usabilidad.

Barra de herramientas del escritorio

Los usuarios ahora pueden acceder a la barra de herramientas del **escritorio** tanto en modo de ventana como en modo de pantalla completa. Antes, la barra de herramientas solo estaba visible en el modo de pantalla completa. Otros cambios en la barra de herramientas incluyen:


- El botón **Inicio** se ha quitado de la barra de herramientas. Esta función se puede ejecutar mediante los comandos siguientes:
 - Cmd-Tab para cambiar a la aplicación activa anterior.
 - Ctrl-Flecha izquierda para cambiar al espacio anterior.
 - Mediante el trackpad integrado o gestos de Magic Mouse para cambiar a un espacio diferente.
 - Al mover el cursor hacia el borde de la pantalla cuando se está en modo de pantalla completa, aparece un Dock donde se puede elegir las aplicaciones que se quiere activar.
- El botón **En una ventana** se ha quitado de la barra de herramientas. Siga uno de estos métodos para cambiar del modo de pantalla completa al modo de ventana:
 - En OS X 10.10, haga clic en el botón de ventana verde de la barra de menú desplegable.
 - En OS X 10.9, haga clic en el botón de menú azul de la barra de menú desplegable.
 - En todas las versiones de OS X, seleccione **Salir de pantalla completa** en el menú **Visualización** de la barra de menú desplegable.
- Función para el arrastre entre ventanas en pantalla completa con varios monitores.

Control del espacio de trabajo

El control del espacio de trabajo permite que las aplicaciones sigan disponibles para los usuarios cuando estos cambian de dispositivo. Por ejemplo, que los médicos en los hospitales se trasladen de una estación de trabajo a otra sin tener que reiniciar sus escritorios ni aplicaciones en cada dispositivo.

Las directivas y asignaciones de las unidades del cliente cambian cuando se traslada a un dispositivo de usuario nuevo. Las directivas y asignaciones se aplican de acuerdo con el dispositivo de usuario donde se inicia la sesión. Por ejemplo, un trabajador sanitario puede cerrar sesión en un dispositivo de la sala de emergencias e iniciar sesión en una estación de trabajo del laboratorio de rayos X. Las directivas, las asignaciones de impresora y las asignaciones de unidades de cliente correspondientes de la sesión en el laboratorio de rayos X entran en vigor para la sesión en el laboratorio de rayos X.

Para configurar los parámetros de control del espacio de trabajo

1. Haga clic en el  en la ventana de la aplicación Citrix Workspace para Mac y elija **Preferencias**.
2. Haga clic en la ficha **General**.
3. Elija una de las siguientes opciones:
 - Reconectar aplicaciones al iniciar la aplicación Citrix Workspace. Permite que los usuarios se vuelvan a conectar a aplicaciones desconectadas cuando inician la aplicación Citrix Workspace.
 - Reconectar aplicaciones al iniciar o actualizar las aplicaciones. Permite que los usuarios se vuelvan a conectar a aplicaciones desconectadas cuando inician las aplicaciones o cuando seleccionan Actualizar aplicaciones en el menú de la aplicación Citrix Workspace para Mac.


Asignación de unidades del cliente

La asignación de unidades del cliente permite acceder a las unidades locales en el dispositivo de usuario como las unidades de CD-ROM, DVD y los dispositivos de memoria USB durante las sesiones. Cuando la configuración de un servidor permite la asignación de unidades del cliente, los usuarios pueden acceder a los archivos almacenados localmente y trabajar en ellos durante las sesiones. Los usuarios también pueden guardarlos en una unidad local o en una unidad del servidor.

La aplicación Citrix Workspace para Mac supervisa los directorios en los que los dispositivos de hardware como CD-ROM, DVD y dispositivos de memoria USB se montan normalmente en el dispositivo de usuario, y asigna automáticamente los dispositivos nuevos que aparecen durante una sesión a la siguiente letra de unidad disponible en el servidor.

Es posible configurar el nivel de acceso de lectura y escritura para las unidades asignadas mediante las preferencias de la aplicación Citrix Workspace para Mac.

Para configurar el acceso de lectura y escritura de las unidades asignadas

1. En la página de inicio de la aplicación Citrix Workspace para Mac, haga clic en el  y seleccione **Preferencias**.
2. Haga clic en **Acceso a archivos**.
3. Seleccione el nivel de acceso de lectura y escritura para las unidades asignadas mediante las siguientes opciones:
 - Lectura y escritura
 - Solo lectura
 - Sin acceso
 - Preguntar siempre
4. Cierre las sesiones abiertas y vuelva a conectarse para aplicar los cambios.

Almacén web personalizado

Puede acceder al almacén web personalizado de su organización desde la aplicación Citrix Workspace para Mac. Para usar esta función, el administrador debe agregar el almacén web personalizado a la lista de URL permitidas en la propiedad `allowedWebStoreURLs` de Global App Configuration Service.

Para obtener más información sobre cómo configurar las direcciones URL de almacén web para los usuarios finales, consulte [Global App Configuration Service](#).

Para agregar una URL de almacén web personalizado, siga estos pasos:

1. Abra la aplicación Workspace y vaya a **Cuentas**.
2. En la ventana **Cuentas**, haga clic en el icono **+** y escriba la URL.

Para eliminar una URL de almacén web personalizado, siga estos pasos:

1. Abra la aplicación Workspace y vaya a **Cuentas**.
2. En la ventana **Cuentas**, seleccione la cuenta que quiera eliminar y haga clic en el icono **-**.

Autenticarse

February 11, 2022

Tarjeta inteligente

La aplicación Citrix Workspace para Mac admite la autenticación con tarjeta inteligente en las configuraciones siguientes:

- Autenticación con tarjeta inteligente en Workspace para Web o StoreFront 2.x y versiones posteriores
- Citrix Virtual Apps and Desktops 7 1808 y versiones posteriores
- XenDesktop 7.1 y versiones posteriores o XenApp 6.5 y versiones posteriores
- Aplicaciones habilitadas para tarjeta inteligente, como Microsoft Outlook y Microsoft Office, que permiten a los usuarios firmar o cifrar digitalmente los documentos disponibles en las sesiones de aplicación o escritorio virtual.
- La aplicación Citrix Workspace para Mac admite múltiples certificados con una única tarjeta inteligente o con varias de ellas. Cuando el usuario introduce una tarjeta inteligente en el lector de tarjetas, los certificados están disponibles para todas las aplicaciones ejecutadas en el dispositivo, incluida la aplicación Citrix Workspace para Mac.
- En sesiones de doble salto, se establece una conexión adicional entre la aplicación Citrix Workspace para Mac y el escritorio virtual del usuario.

Acerca de la autenticación con tarjetas inteligentes para acceder a Citrix Gateway

Existen varios certificados que se pueden utilizar al usar una tarjeta inteligente para autenticar una conexión. La aplicación Citrix Workspace para Mac le pide que seleccione un certificado. Tras seleccionar un certificado, la aplicación Citrix Workspace para Mac solicita la contraseña de la tarjeta inteligente. Una vez autenticada, se inicia la sesión.

Si solo hay un certificado adecuado en la tarjeta inteligente, la aplicación Citrix Workspace para Mac usa ese certificado y no pide seleccionarlo. No obstante, aún hay que introducir la contraseña asociada con la tarjeta inteligente para autenticar la conexión y que se inicie la sesión.

Especificación de un módulo PKCS#11 para la autenticación con tarjeta inteligente

Nota:

La instalación del módulo PKCS#11 no es obligatoria. Esta sección se aplica solo a las sesiones ICA. No se aplica el acceso de Citrix Workspace a Citrix Gateway o StoreFront donde se necesita una tarjeta inteligente.

Para especificar el módulo PKCS#11 para la autenticación con tarjeta inteligente:

1. Seleccione **Preferencias** en la aplicación Citrix Workspace para Mac.
2. Haga clic en **Seguridad y privacidad**.
3. En la sección **Seguridad y privacidad**, haga clic en **Tarjeta inteligente**.
4. En el campo **PKCS#11**, seleccione el módulo apropiado. Haga clic en **Otros** para buscar la ubicación del módulo PKCS#11 si el módulo que quiere usar no aparece en la lista.
5. Después de seleccionar el módulo apropiado, haga clic en **Agregar**.

Perfiles de tarjeta inteligente, middleware y lectores compatibles

La aplicación Citrix Workspace para Mac admite la mayoría de los lectores de tarjeta inteligente y middleware criptográfico compatibles con macOS. Citrix ha validado esta operación con los siguientes dispositivos.

Lectores admitidos:

- Lectores de tarjeta inteligente de conexión USB comunes

Middleware compatible:

- Clarify
- Versión del cliente de ActivIdentity
- Versión del cliente de Charismathics

Tarjetas inteligentes compatibles:

- Tarjetas PIV
- Tarjetas CAC (Common Access Card)
- Tarjetas Gemalto .NET

Siga las instrucciones del proveedor del middleware criptográfico y lector de tarjeta inteligente compatibles con macOS para configurar los dispositivos de usuario.

Restricciones

- Los certificados deben guardarse en una tarjeta inteligente, no en el dispositivo del usuario.
- La aplicación Citrix Workspace para Mac no guarda la selección de certificado de usuario.
- La aplicación Citrix Workspace para Mac no guarda ni almacena el PIN de la tarjeta inteligente del usuario. Las adquisiciones del PIN son gestionadas por el sistema operativo, que tal vez tenga su propio mecanismo de almacenamiento en caché.
- La aplicación Citrix Workspace para Mac no se reconecta a sesiones cuando se inserta una tarjeta inteligente.
- Para utilizar túneles VPN con autenticación de tarjeta inteligente, debe instalar Citrix Gateway Plug-in e iniciar sesión a través de una página web. Utilice sus tarjetas inteligentes y sus PIN para autenticarse en cada paso. La autenticación PassThrough en StoreFront con Citrix Gateway Plug-in no está disponible para los usuarios de tarjeta inteligente.

Proteger comunicaciones

February 11, 2022

Para proteger la comunicación entre el sitio y la aplicación Citrix Workspace para Mac, puede integrar las conexiones con la ayuda de diversas tecnologías de seguridad, incluido Citrix Gateway. Para obtener información sobre cómo configurar Citrix Gateway con Citrix StoreFront, consulte la documentación de

[StoreFront](#).

Nota:

Citrix recomienda utilizar Citrix Gateway para proteger las comunicaciones entre los servidores StoreFront y los dispositivos de los usuarios.

- Un servidor proxy SOCKS o un servidor proxy de seguridad (también conocido como servidor proxy seguro o servidor proxy HTTPS). Se pueden utilizar servidores proxy para limitar el acceso hacia y desde la red, y para gestionar las conexiones entre Citrix Workspace y los servidores. La aplicación Citrix Workspace para Mac admite el uso de SOCKS y protocolos de proxy seguro.
- Citrix Secure Web Gateway. Puede utilizar Citrix Secure Web Gateway para proporcionar un punto de acceso único, seguro y cifrado a Internet para los servidores situados en las redes internas de la organización.
- Soluciones de Traspaso SSL con protocolos TLS (Transport Layer Security)
- Un firewall. Los firewall o servidores de seguridad de red pueden permitir o bloquear los paquetes basándose en la dirección y el puerto de destino. Si usa un firewall que asigna la dirección IP interna del servidor a una dirección de Internet externa, como la traducción de direcciones de red (NAT), configure la dirección externa.

Nota:

A partir de macOS Catalina, Apple ha impuesto requisitos adicionales para los certificados de CA raíz y los certificados intermedios que los administradores deben configurar. Para obtener más información, consulte el artículo [HT210176](#) de la página de soporte de Apple.

Citrix Gateway

Para permitir a los usuarios remotos conectarse a su implementación de XenMobile a través de Citrix Gateway, puede configurar Citrix Gateway para que admita StoreFront. El método que se debe utilizar para habilitar el acceso depende de la edición de XenMobile existente en la implementación.

Si implementa XenMobile en la red, integre Citrix Gateway en StoreFront para permitir las conexiones de usuarios internos y usuarios remotos a StoreFront a través de Citrix Gateway. Con esta implementación, los usuarios pueden conectarse a StoreFront para acceder a las aplicaciones publicadas desde XenApp y a los escritorios virtuales desde XenDesktop. Los usuarios se pueden conectar mediante la aplicación Citrix Workspace.

Conexión con Citrix Secure Web Gateway

Si se instala Citrix Secure Web Gateway Proxy en un servidor de una red segura, se puede utilizar Citrix Secure Web Gateway Proxy en modo de traspaso (Relay). Para obtener más información acerca del modo Relay, consulte la documentación de [XenApp y Citrix Secure Web Gateway](#).

Si se utiliza el modo de traspaso, el servidor Citrix Secure Web Gateway funciona como un proxy y es necesario configurar la aplicación Citrix Workspace para Mac para que use lo siguiente:

- El nombre de dominio completo (FQDN) del servidor de Citrix Secure Web Gateway.
- El número de puerto del servidor de Citrix Secure Web Gateway. La versión 2.0 de Citrix Secure Web Gateway no ofrece el modo de traspaso.

El nombre de dominio completo (FQDN) debe tener los siguientes tres componentes, consecutivamente:

- Nombre de host
- Dominio intermedio
- Dominio superior

Por ejemplo, `mi_equipo.ejemplo.com` es un nombre de dominio completo (FQDN), ya que contiene una secuencia de nombre de host (`mi_equipo`), dominio intermedio (`ejemplo`) y dominio superior (`com`). La combinación del dominio intermedio y del dominio superior (`example.com`) se denomina “nombre de dominio”.

Conexión a través de un servidor proxy

Los servidores proxy se usan para limitar el acceso hacia y desde una red, y para ocuparse de las conexiones entre la aplicación Citrix Workspace para Mac y los servidores. La aplicación Citrix Workspace para Mac admite el uso de SOCKS y protocolos de proxy seguro.

Cuando la aplicación Workspace para Mac se comunica con el servidor web, utiliza los parámetros del servidor proxy configurados para el explorador web predeterminado en el dispositivo de usuario. Configure los parámetros del servidor proxy para el explorador web predeterminado en el dispositivo de usuario según corresponda.

Conexión a través de un firewall

Los firewall o servidores de seguridad de red pueden permitir o bloquear los paquetes basándose en la dirección y el puerto de destino. La aplicación Citrix Workspace para Mac debe poder comunicarse a través del firewall con el servidor web y el servidor de Citrix. El firewall debe permitir el tráfico HTTP para la comunicación entre el dispositivo de usuario y el servidor web (normalmente mediante un puerto HTTP 80 o 443 estándar para un servidor web seguro). Para las comunicaciones entre Citrix Workspace y el servidor Citrix, el firewall debe permitir el tráfico ICA entrante en los puertos 1494 y 2598.

TLS

Transport Layer Security (TLS) es la versión estándar más reciente del protocolo TLS. La organización Internet Engineering Taskforce (IETF) le cambió el nombre a TLS al asumir la responsabilidad del desarrollo de TLS como un estándar abierto.

TLS protege las comunicaciones de datos mediante la autenticación del servidor, el cifrado del flujo de datos y la comprobación de la integridad de los mensajes. Algunas organizaciones, entre las que se encuentran organizaciones del gobierno de los EE. UU., requieren el uso de TLS para proteger las comunicaciones de datos. Es posible que estas organizaciones también exijan el uso de cifrado válido, como FIPS 140 (Federal Information Processing Standard). FIPS 140 es un estándar para cifrado.

La aplicación Citrix Workspace para Mac admite claves RSA de 1024, 2048 y 3072 bits. También se admiten certificados raíz con claves RSA de 4096 bits.

Nota

La aplicación Citrix Workspace para Mac usa criptografía de plataforma (OS X) para las conexiones entre aplicación Citrix Workspace para Mac y StoreFront.

Estos conjuntos de cifrado se han retirado para mejorar la seguridad:

- Conjuntos de cifrado con el prefijo “TLS_RSA_”
- Conjuntos de cifrado RC4 y 3DES
- TLS_RSA_WITH_AES_256_GCM_SHA384 (0x009d)
- TLS_RSA_WITH_AES_128_GCM_SHA256 (0x009c)
- TLS_RSA_WITH_AES_256_CBC_SHA256 (0x003d)
- TLS_RSA_WITH_AES_256_CBC_SHA (0x0035)
- TLS_RSA_WITH_AES_128_CBC_SHA (0x002f)
- TLS_RSA_WITH_RC4_128_SHA (0x0005)
- TLS_RSA_WITH_3DES_EDE_CBC_SHA (0x000a)

La aplicación Citrix Workspace para Mac solo admite los siguientes conjuntos de cifrado:

- TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 (0xc030)
- TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384 (0xc028)
- TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA (0xc013)

Para los usuarios de DTLS 1.0, la aplicación Citrix Workspace para Mac 1910 y versiones posteriores solo admiten este conjunto de cifrado:

- TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA (0xc013)

Actualice la versión de Citrix Gateway a 12.1 o a una posterior si quiere utilizar DTLS 1.0. De lo contrario, recurre a TLS en función de la directiva DDC.

Las siguientes tablas proporcionan detalles de las conexiones de red internas y externas:

Client cipher set	VDA cipher set	Direct connections								
		TLS			DTLS v1.0			DTLS v1.2		
		Open	FIPS	SP800-52	Open	FIPS	SP800-52	Open	FIPS	SP800-52
Any	ANY	Y	Y	Y	Y			Y		
	COM	Y	X	X	Y			Y		
	GOV	Y	Y	Y	Y			Y		
COM	ANY	Y	X	X	Y					
	COM	Y	X	X	Y					
	GOV	Y	X	X	Y					
GOV	ANY	Y	Y	Y	X			Y		
	COM	X	X	X	X			X		
	GOV	Y	Y	Y	X			Y		

Client cipher set	VDA cipher set	External connections with Citrix Gateway								
		TLS			DTLS v1.0			DTLS v1.2		
		Open	FIPS	SP800-52	Open	FIPS	SP800-52	Open	FIPS	SP800-52
Any	ANY	Y	Y	Y	Y			X		
	COM	Y	X	X	Y			X		
	GOV	Y	Y	Y	Y			X		
COM	ANY	Y	X	X	Y			X		
	COM	Y	X	X	Y			X		
	GOV	Y	X	X	Y			X		
GOV	ANY	Y	Y	Y	X			X		
	COM	X	X	X	X			X		
	GOV	Y	Y	Y	X			X		

Nota:

- Utilice Citrix Gateway 12.1 o una versión más reciente para que EDT funcione correctamente. Las versiones anteriores no admiten conjuntos de cifrado ECDHE en modo DTLS.
- Citrix Gateway no es compatible con DTLS 1.2. Por lo tanto, `TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384` y `TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384` no son compatibles. Citrix Gateway debe configurarse para que use `TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA` de modo que funcione correctamente en DTLS 1.0.

Configurar y habilitar la aplicación Citrix Workspace para TLS

La configuración de TLS consta de dos pasos:

1. Configure el Traspaso SSL en el servidor de Citrix Virtual Apps and Desktops y obtenga e instale el certificado de servidor necesario.

2. Instale el certificado raíz equivalente en el dispositivo de usuario.

Instalación de certificados raíz en los dispositivos de los usuarios

Si se quiere usar TLS para proteger la seguridad de las comunicaciones entre las instancias de la aplicación Citrix Workspace para Mac habilitadas con TLS y la comunidad de servidores, se necesita un certificado raíz en el dispositivo de usuario. Este certificado raíz verifica la firma de la entidad emisora de certificación en el certificado del servidor.

macOS X viene con unos 100 certificados raíz comerciales ya instalados. Sin embargo, si quiere utilizar otro certificado, puede obtenerlo de la entidad de certificación e instalarlo en cada dispositivo de usuario.

Instale el certificado raíz en cada dispositivo, según las directivas y los procedimientos de su organización, en lugar de solicitar a los usuarios que lo instalen. La opción más fácil y segura es agregar los certificados raíz a las llaves de macOS X.

Para agregar un certificado raíz a las llaves

1. Haga doble clic en el archivo que contiene el certificado. Esta acción inicia automáticamente la aplicación Acceso a Llaveros.
2. En el cuadro de diálogo Añadir certificados, elija una de las siguientes opciones en el menú emergente Llaveros:
 - Inicio de sesión (el certificado se aplica solamente al usuario actual).
 - Sistema (el certificado se aplica a todos los usuarios de un dispositivo).
3. Haga clic en Aceptar.
4. Escriba su contraseña en el cuadro de diálogo Autenticar y haga clic en Aceptar.

Se instalará el certificado raíz, y los clientes compatibles con TLS y todas las aplicaciones que utilicen TLS lo usarán.

Acerca de las directivas de TLS

Esta sección proporciona información sobre cómo configurar directivas de seguridad para sesiones ICA sobre TLS. Puede configurar ciertos parámetros de TLS utilizados para las conexiones ICA en la aplicación Citrix Workspace para Mac. Estos parámetros no se exponen en la interfaz de usuario. Para cambiarlos, es necesario ejecutar un comando en el dispositivo que tiene la aplicación Citrix Workspace para Mac.

Nota

Las directivas TLS se administran de otras maneras; por ejemplo, con dispositivos controlados por un servidor de OS X o con otra solución de administración de dispositivos móviles.

Las directivas TLS incluyen los siguientes parámetros:

SecurityComplianceMode. Define el modo de conformidad de seguridad para la directiva. Si no se configura SecurityComplianceMode, se usa FIPS como valor predeterminado. Los valores aplicables para este parámetro son:

- **None.** No se impone ningún modo de conformidad
- **FIPS.** Se usan módulos criptográficos de FIPS
- **SP800-52.** Se imponen las normas de conformidad NIST SP800-52r1

```
defaults write com.citrix.receiver.nomas SecurityComplianceMode SP800-52
```

SecurityAllowedTLSVersions. Especifica las versiones del protocolo TLS que se aceptan durante la negociación de protocolos. Esta información está representada por una matriz y se admite cualquier combinación de los valores posibles. Cuando este parámetro no está configurado, se usan los valores TLS10, TLS11 y TLS12 como valores predeterminados. Los valores aplicables para este parámetro son:

- **TLS10.** Especifica que se permite el protocolo TLS 1.0.
- **TLS11.** Especifica que se permite el protocolo TLS 1.1.
- **TLS12.** Especifica que se permite el protocolo TLS 1.2.

```
defaults write com.citrix.receiver.nomas SecurityAllowedTLSVersions -array  
TLS11 TLS12
```

SSLCertificateRevocationCheckPolicy. Mejora la autenticación criptográfica del servidor de Citrix y mejora la seguridad global de las conexiones SSL/TLS entre clientes y servidores. Este parámetro rige la gestión de una entidad de certificación (CA) raíz de confianza al abrir una sesión remota a través de SSL cuando se usa el cliente para OS X.

Cuando se habilita este parámetro, el cliente comprueba si el certificado del servidor está revocado. Existen varios niveles de comprobación de la lista de revocación de certificados. Por ejemplo, se puede configurar el cliente para que verifique solo la lista local de certificados, o para que compruebe las listas de certificados locales y de red. Además, se puede configurar la comprobación de certificados para permitir que los usuarios inicien sesiones solo cuando se hayan comprobado todas las listas de revocación de certificados.

La comprobación de listas de revocación de certificados (listas CRL) es una funcionalidad avanzada admitida por algunos emisores de certificados. Permite a los administradores revocar certificados de seguridad (no válidos una vez transcurrida su fecha de caducidad) si existe un riesgo criptográfico para las claves privadas del certificado o si ha habido cambios inesperados en el nombre DNS.

Los valores aplicables para este parámetro son:

- **NoCheck.** No comprueba la lista de revocación de certificados.

- **CheckWithNoNetworkAccess.** Se hace una comprobación de listas de revocación de certificados. Solo se usan almacenes locales de listas de revocación de certificados. Se ignoran todos los puntos de distribución. No es obligatorio encontrar una lista de revocación de certificados para la verificación del certificado del servidor presentado por el servidor de Traspaso SSL/Citrix Secure Web Gateway de destino.
- **FullAccessCheck.** Se hace una comprobación de listas de revocación de certificados. Se utilizan los almacenes locales de listas de revocación de certificados y todos los puntos de distribución. No es obligatorio encontrar una lista de revocación de certificados para la verificación del certificado del servidor presentado por el servidor de Traspaso SSL/Citrix Secure Web Gateway de destino.
- **FullAccessCheckAndCRLRequired.** Se lleva a cabo la comprobación de la lista de revocación de certificados y se excluye la entidad de certificación raíz. Se utilizan los almacenes locales de listas de revocación de certificados y todos los puntos de distribución. Para la verificación, es necesario encontrar todas las listas de revocación de certificados requeridas.
- **FullAccessCheckAndCRLRequiredAll.** Se lleva a cabo la comprobación de la lista de revocación de certificados y se incluye la entidad de certificación raíz. Se utilizan los almacenes locales de listas de revocación de certificados y todos los puntos de distribución. Para la verificación, es necesario encontrar todas las listas de revocación de certificados requeridas.

Nota

Si no se configura `SSLCertificateRevocationCheckPolicy`, el valor predeterminado que se usa es “FullAccessCheck”.

```
defaults write com.citrix.receiver.nomas SSLCertificateRevocationCheckPolicy  
FullAccessCheckAndCRLRequired
```

Configuración de directivas TLS

Para configurar los parámetros de TLS en un equipo no administrado, ejecute el comando **defaults** en Terminal.app.

defaults es una aplicación de línea de comandos que se puede usar para agregar, modificar y eliminar parámetros de aplicación en un archivo de lista de preferencias de OS X.

Para cambiar parámetros:

1. Abra **Aplicaciones > Utilidades \ > Terminal**.
2. En Terminal, ejecute el comando:

```
defaults write com.citrix.receiver.nomas <name> <type> <value>
```

Donde:

<name>: El nombre del parámetro según se describe más arriba.

<type>: Un conmutador que identifica el tipo de parámetro. Puede ser `-string` o `-array`. Si el tipo de parámetro es una cadena, este parámetro se puede omitir.

<value>: El valor del parámetro. Si el valor es una matriz y es necesario especificar varios valores, sepárelos con un espacio.

```
defaults write com.citrix.receiver.nomas SecurityAllowedTLSVersions -array  
TLS11 TLS12
```

Volver a la configuración predeterminada

Para restablecer un parámetro con su valor predeterminado:

1. Abra **Aplicaciones > Utilidades \ > Terminal**.
2. En Terminal, ejecute el comando:

```
defaults delete com.citrix.receiver.nomas <name>
```

Donde:

<name>: El nombre del parámetro según se describe más arriba.

```
defaults delete com.citrix.receiver.nomas SecurityAllowedTLSVersions
```

Parámetros de seguridad

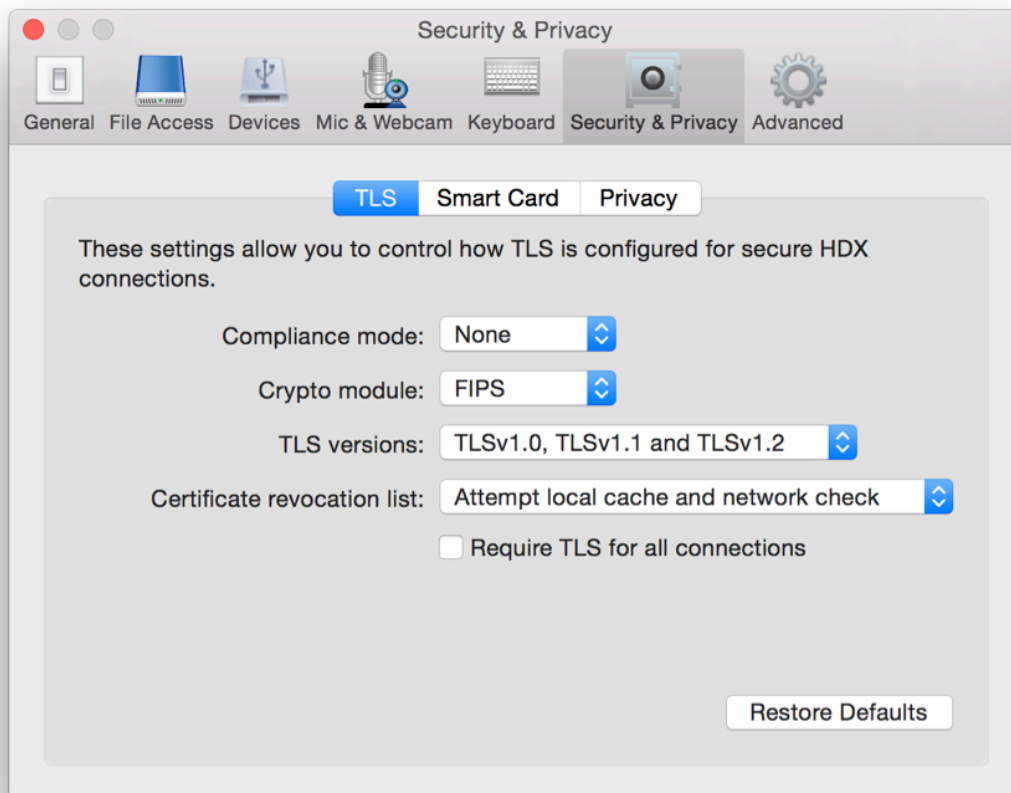
En la versión 12.3 de Citrix Receiver para Mac se incorporaron varias mejoras generales y de seguridad, que incluyen lo siguiente:

- Interfaz de usuario de configuración de seguridad mejorada. En versiones anteriores, la línea de comandos era el método preferido para realizar cambios relacionados con la seguridad. Ahora, los parámetros de configuración relacionados con la seguridad de las sesiones son sencillos y accesibles desde la interfaz de usuario. Esta mejora contribuye a la experiencia de usuario y crea un método intuitivo para la adopción de preferencias relacionadas con la seguridad.
- Ver conexiones TLS. Puede verificar conexiones que usen versiones de TLS, algoritmos de cifrado, modos, tamaños de clave y estados específicos de SecureICA. Además, puede ver el certificado del servidor para las conexiones TLS.

La pantalla mejorada de **Seguridad y privacidad** ofrece las siguientes opciones nuevas en la ficha **TLS**:

- Definir el modo de conformidad
- Configurar el módulo de criptografía
- Seleccionar la versión de TLS adecuada
- Seleccionar la lista de revocación de certificados
- habilitar parámetros para todas las conexiones TLS

En la imagen siguiente, aparecen las opciones de la pantalla **Seguridad y privacidad** a las que se puede acceder desde la interfaz de usuario:



**Locations**

Corporate Headquarters | 851 Cypress Creek Road Fort Lauderdale, FL 33309, United States
Silicon Valley | 4988 Great America Parkway Santa Clara, CA 95054, United States

© 2022 Citrix Systems, Inc. All rights reserved. Citrix, the Citrix logo, and other marks appearing herein are property of Citrix Systems, Inc. and/or one or more of its subsidiaries, and may be registered with the U.S. Patent and Trademark Office and in other countries. All other marks are the property of their respective owner(s).