Aplicación Citrix Workspace para Mac

Contents

Acerca de esta versión

April 12, 2021

> **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 asistencia de Apple.

Novedades en la versión 2104

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 el inicio de sesión único 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 acerca de la configuración de recursos compartidos de red, consulte Crear y administrar conectores de zonas de almacenamiento.

Novedades en la versión 2102

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

Novedades en la versión 2101

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 acerca de Rosetta, consulte el artículo de soporte técnico 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.

Novedades en la versión 2012

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.

Novedades en la versión 2010

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 de modo que no es necesario volver a introducir las credenciales en caso de que se reinicie el sistema o se reinicie 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.

Novedades en la versión 2009

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.

Novedades en la versión 2008

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.

Novedades en la versión 2007

Mejoras en el rendimiento

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

Novedades en la versión 2006

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 Autoservicio para el rendimiento y Búsqueda de autoservicio para 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 una serie de problemas para mejorar la estabilidad general.

Novedades en la versión 2005

Idiomas disponibles

Ahora la aplicación Citrix Workspace para Mac está disponible en italiano.

Mejoras en el rendimiento

- En esta versión se han resuelto varios problemas para mejorar la estabilidad y el rendimiento generales en Citrix Workspace (almacenes en la nube).
- Con esta versión, los usuarios de la nube notarán tiempos de inicio de sesión más cortos y tiempos de enumeración de aplicaciones más cortos.

Novedades en la versión 2002

Claves de 4096 bits en modo FIPS

Ahora la aplicación Citrix Workspace para Mac admite claves RSA de 4096 bits en el modo criptográfico Federal Information Processing Standard Publication (FIPS 140).

Mejoras en el rendimiento

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

Novedades en 2001

Protección de aplicaciones

La aplicación Citrix Workspace para Mac admite ahora la protección de aplicaciones. La protección de aplicaciones es una función adicional que proporciona una mayor seguridad al usar Citrix Virtual Apps and Desktops. La función restringe la posibilidad de que los clientes puedan verse amenazados por malware de registro de pulsaciones de teclas y malware de capturas de pantalla. La protección de aplicaciones evita la exfiltración de información confidencial, como credenciales de usuario e información confidencial mostrada en la pantalla. La función evita que los usuarios y los atacantes hagan capturas de pantalla y usen registradores de pulsaciones de teclas para obtener y explotar información confidencial. Para obtener información sobre la configuración de la protección de aplicaciones en Citrix Virtual Apps and Desktops, consulte Protección de aplicaciones.

Problemas conocidos y limitaciones:

Para que esta función opere correctamente, inhabilite la directiva **Redirección del portapapeles del cliente** del VDA.

Idiomas disponibles

La aplicación Citrix Workspace para Mac ya está disponible en portugués (Brasil).

Carga mejorada de canales virtuales de terceros

La aplicación Citrix Workspace para Mac admite ahora una carga mejorada de canales virtuales de terceros. Esto mejora la experiencia del usuario de las siguientes maneras:

- No es necesario volver a instalar los canales virtuales de terceros (por ejemplo, RealTime Media Engine) al desinstalar y volver a instalar la aplicación Citrix Workspace.
- Los usuarios con privilegios de cuenta estándar también pueden disfrutar de una experiencia optimizada con RealTime Optimization Pack incluso cuando un administrador haya instalado su motor RealTime Media Engine.

Novedades en la versión 1912

Workspace con funciones inteligentes

Esta versión de la aplicación Citrix Workspace para Mac está optimizada para aprovechar las próximas funciones inteligentes cuando se publiquen. Para obtener más información, consulte Funciones inteligentes de Workspace: Microaplicaciones.

Novedades en 1910.2

Esta versión resuelve problemas con Actualizaciones de Citrix Workspace y macOS Catalina.

- Los clientes que utilicen la aplicación Citrix Workspace 1910 y 1910.1 para Mac deben actualizar la versión a la 1910.2 manualmente para recibir actualizaciones futuras a través de Actualizaciones de Citrix Workspace.
- Los clientes que utilizan la aplicación Citrix Workspace 1906 para Mac o versiones anteriores pueden obtener la aplicación Citrix Workspace 1910.2 para Mac a través de Actualizaciones de Citrix Workspace.

Novedades en la versión 1910.1

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

Novedades en la versión 1910

Compatibilidad con macOS Catalina

La aplicación Citrix Workspace para Mac se puede utilizar en macOS Catalina.

> **Nota:**
>
> Al abrir la aplicación Citrix Workspace para Mac y Citrix Viewer por primera vez en macOS Catalina, el sistema operativo solicita a los usuarios que permitan las notificaciones de Citrix Viewer. Haga clic en **Permitir** para recibir notificaciones relacionadas con la aplicación Citrix Workspace para Mac.

Actualización de los conjuntos de cifrado

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 solo admite este conjunto de cifrado:

- TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA (0xc013)

Citrix recomienda actualizar la versión de NetScaler 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. Para obtener más información, consulte el artículo CTX250104 de Knowledge Center.

Actualizaciones de Citrix Casting

Ahora Citrix Casting se desconecta automáticamente cuando los usuarios cierran la tapa del portátil.

Novedades en la versión 1906

Actualizaciones de Citrix Casting

Controle la sesión en Citrix Ready Workspace Hub mediante dispositivos periféricos. Ahora puede usar el teclado y el mouse tanto en el hub como en el dispositivo para administrar la sesión. Para obtener más información, consulte Citrix Ready Workspace Hub.

Idiomas disponibles

La aplicación Citrix Workspace para Mac ahora está disponible en neerlandés.

Novedades en la versión 1903.1

Actualizaciones de Citrix Casting

Citrix Casting se ha actualizado con nuevas funciones y mejoras. Para obtener más información sobre Citrix Casting, consulte Citrix Casting.

Novedades en la versión 1901

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

Novedades en la versión 1812

Citrix Casting

Citrix Casting se utiliza para proyectar la pantalla de su Mac en dispositivos cercanos de Citrix Ready Workspace Hub. En esta versión, se admite la duplicación de la pantalla de su Mac en monitores conectados al Workspace Hub.

Para obtener más información sobre Citrix Casting, consulte Configuración de Citrix Casting.

Sincronización de la distribución de teclado

A partir de esta versión, la aplicación Citrix Workspace para Mac ofrece una sincronización dinámica de la distribución del teclado desde el cliente al Linux VDA en una sesión. Esto permite a los usuarios cambiar entre sus distribuciones de teclado preferidas en el dispositivo cliente, lo que proporciona una experiencia de usuario uniforme cuando, por ejemplo, cambian de una distribución de teclado en inglés a español.

Para obtener más información sobre la configuración de la distribución del teclado, consulte Distribución del teclado. Para obtener más información sobre cómo configurar la sincronización de distribución del teclado en los Linux VDA, consulte Sincronización de la distribución de teclado dinámico.

Experiencia de IME de cliente mejorada

A partir de esta versión, la aplicación Citrix Workspace para Mac ofrece una mejor experiencia de usuario con las entradas IME del cliente y los Linux VDA. Con esta funcionalidad, podrá ver dos mejoras en la entrada del IME del cliente:

- La ventana de candidatos que contiene la lista de caracteres de composición siempre aparece junto al punto de inserción, en lugar de aparecer en la esquina inferior izquierda, que era su ubicación anterior.
- Los caracteres compuestos que se muestran en el VDA están marcados para que el usuario no los confunda con los caracteres determinados.

Esta función depende de la funcionalidad de sincronización de distribución de teclado.

Para obtener más información sobre cómo configurar esta mejora de IME del cliente, consulte IME de cliente mejorada. Para obtener más información sobre cómo configurar el IME del cliente en Linux VDA, consulte Sincronización de la interfaz de usuario IME del cliente.

Selective H264

Selective H264 permite que las partes de la pantalla que cambian rápidamente, como sucede al reproducir un vídeo, se reciban como un streaming H264. Para habilitar H264 selectivo, establezca la directiva **Usar códec de vídeo para compresión** en **Para regiones que cambian activamente**.

Novedades en la versión 1809

Compatibilidad con macOS Mojave

La aplicación Citrix Workspace para Mac es totalmente compatible con macOS Mojave, incluido el modo oscuro.

Compatibilidad con WebApp

La aplicación Secure Browser para Citrix Workspace para Mac ahora admite cookies y redirecciones cuando se utiliza Citrix Gateway.

Novedades en la versión 1808

Compatibilidad con 64 bits

Ahora la aplicación Citrix Workspace para Mac es totalmente de 64 bits.

> **Nota:**
>
> Los usuarios que actualicen a la aplicación Citrix Workspace no tendrán una experiencia de Skype Empresarial (Lync) optimizada debido a una falta de coincidencia de bits. La aplicación Citrix Workspace para Mac es de 64 bits, mientras que la versión actualmente instalada de RTME es de 32 bits. Como solución temporal, considere usar la versión de acceso anticipado de RTME.
>
> **Nota:**
>
> Los canales virtuales personalizados de 32 bits ya no funcionan y deben actualizarse a 64 bits.

Autenticación federada

Ahora la aplicación Citrix Workspace para Mac admite la autenticación federada a través de Azure Active Directory.

Mostrar u ocultar la barra de idioma remota

A partir de esta versión, puede optar por mostrar u ocultar la barra de idioma remota en una sesión de aplicación mediante la interfaz gráfica de usuario. La barra de idioma muestra el idioma de entrada preferido en una sesión. En versiones anteriores, solo puede cambiar esta configuración mediante

las claves de Registro en el VDA. A partir de la versión 1808 de la aplicación 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.

Para obtener más información, consulte Configuración y el artículo CTX231913 de Knowledge Center.

> **Nota:**
>
> Esta función está disponible en sesiones que se ejecutan en VDA 7.17 y versiones posteriores.

Soporte para Citrix Analytics

La aplicación Citrix Workspace está equipada para transmitir registros de manera segura a Citrix Analytics. Los registros se analizan y almacenan en Citrix Analytics cuando está habilitado. Para obtener más información sobre Citrix Analytics, consulte la documentación de Citrix Analytics.

Problemas resueltos

Problemas resueltos en la versión 2104

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

Problemas resueltos en la versión 2102

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

Problemas resueltos en la versión 2101

- 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]

Problemas resueltos en la versión 2012

- 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]

Problemas resueltos en la versión 2010

- 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]

Problemas resueltos en la versión 2009

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

Problemas resueltos en la versión 2008

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

Problemas resueltos en la versión 2007

- 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]

Problemas resueltos en la versión 2006

- 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 resueltos en la versión 2005

- Es posible que no se pueda iniciar sesión en la aplicación Citrix Workspace desde macOS Catalina mediante tarjetas inteligentes PIV y que aparezca el mensaje de error: "No se pudo detectar la cuenta especificada". [CVADHELP-14155]
- A veces, es posible que la ventana principal de una instancia publicada de Microsoft Outlook se vuelva negra cuando su ventana modal tiene el foco. [CVADHELP-14169]

Problemas resueltos en la versión 2002

- Es posible que no se puedan iniciar sesiones en la aplicación Citrix Workspace desde macOS Catalina (10.15.2) mediante tarjetas inteligentes PIV y que aparezca el mensaje de error: "One or more root certificates is not valid" (Al menos uno de los certificados raíz no es válido). [RFMAC-3365]
- Es posible que no se pueda escribir en aplicaciones publicadas (como, por ejemplo, el Bloc de notas) con los idiomas chino o japonés establecidos. [RFMAC-3556]

Problemas resueltos en la versión 2001

- Es posible que, al iniciar escritorios publicados con la directiva de profundidad de color máxima de 16 bpp habilitada en un MacBook, muestren una pantalla gris y dejen de responder. [CVADHELP-13605]
- Es posible que no se puedan pegar capturas de pantalla tomadas en la aplicación DingTalk en instancias publicadas de Microsoft Paint y Microsoft Word y que aparezca una pantalla en blanco o un mensaje de error, respectivamente. [CVADHELP-13938]

Problemas resueltos en la versión 1912

- Al utilizar las versiones 1812 o 1901 de la aplicación Citrix Workspace para Mac, el hecho de mover aplicaciones publicadas por la pantalla tarda en responder. [RFMAC-2300]
- Es posible que no se pueda iniciar sesión en la aplicación Citrix Workspace en macOS Catalina mediante tarjetas inteligentes PIV. [RFMAC-2788]
- En la aplicación Citrix Workspace para Mac 1909, al abrir un archivo ICA con nombres que no estén en inglés, es posible que Citrix Viewer se cierre de manera inesperada. [RFMAC-2986]
- Es posible que, al iniciar aplicaciones publicadas de Microsoft Outlook y PowerShell, estas no respondan o tarden en responder tras actualizar la versión de la aplicación Citrix Workspace para Mac. [LD1192]
- Las ventanas de las aplicaciones publicadas no se actualizan o tardan en actualizarse al moverlas por la pantalla. [LD1485]

Problemas corregidos en 1910.2

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

Problemas resueltos en la versión 1910.1

- Al utilizar FaceTime en un MacBook Pro 2018 y versiones posteriores, es posible que los usuarios vean una barra verde en la parte inferior de la vista previa del vídeo. [RFMAC-2317]
- Es posible que no se puedan iniciar sesiones con una tarjeta inteligente a través de Citrix Gateway, tras lo cual aparece el mensaje de error “El homólogo SSL remoto envió una alerta de fallo de negociación”. [RFMAC-2727]
- Cuando la autenticación SAML está habilitada, es posible que la pantalla de autenticación tarde en responder o directamente no responda. Como solución temporal, reinicie el dispositivo. [RFMAC-3047]

- Al denegar el permiso de automatización después de iniciar las aplicaciones suscritas, es posible que la aplicación Citrix Workspace para Mac deje de responder. [RFMAC-3048]

Problemas resueltos en la versión 1910

- Al copiar texto de la aplicación Citrix Workspace para Mac a otra aplicación, es posible que se muestren caracteres incorrectos. [RFMAC-2581]
- Es posible que el inicio de sesión en la aplicación Citrix Workspace para Mac tarde más de lo esperado. [RFMAC-2608]
- El uso de un proxy para conectarse puede provocar que el proxy se cierre de manera inesperada. [RFMAC-2612]
- Cuando se utiliza más de un monitor, es posible que los movimientos del mouse no estén sincronizados en aplicaciones integradas. [RFMAC-2623]
- Al volver a iniciar sesión en la aplicación Citrix Workspace para Mac, es posible que la aplicación se cierre de manera inesperada. [RFMAC-2679]
- Al utilizar la tecla de acceso rápido Comando-Tab para cambiar de ficha, el escritorio virtual deja de responder. [RFMAC-2691]
- Se produce un error al iniciar la aplicación ShareFile cuando la seguridad mejorada está activa. [RFMAC-2724]
- Es posible que Citrix Viewer consuma una cantidad excesiva de CPU. [RFMAC-2777]

Problemas resueltos en la versión 1906

- Es posible que las sesiones de tarjetas inteligentes se desconecten de forma aleatoria. [RFMAC-1816, RFMAC-2313]
- Las sesiones desconectadas pueden provocar que la aplicación Citrix Workspace para Mac deje de responder. [RFMAC-2137]
- La ventana de vista web se muestra sobre todas las aplicaciones. [RFMAC-2146]
- Después de activar un MacBook, la aplicación Citrix Workspace para Mac solicita repetidamente la autenticación. [RFMAC-2161]
- Al iniciar sesión, puede aparecer un error que indica que el servidor no se pudo encontrar. [RFMAC-2192]
- El inicio de una aplicación web sin Single Sign-On configurado puede provocar un error 401, en lugar de solicitar credenciales. [RFMAC-2194]
- Las ventanas de aplicación integradas pueden desaparecer cuando se mueven a un monitor secundario. [RFMAC-2314]
- En ocasiones, podría mostrarse una página de error “No se pudo cargar la página”. [RFMAC-2322]
- Es posible que los usuarios no puedan seleccionar menús al utilizar la aplicación publicada de Microsoft Outlook. [RFMAC-2335]

- Al usar un formulario web, podría mostrarse un error de autenticación. [RFMAC-2349]
- Al intentar conectarse a través de Citrix Gateway y el servidor virtual está configurado para utilizar certificados intermedios firmados, la aplicación Citrix Workspace para Mac se cierra de manera inesperada y se muestra el error SSL 61. [RFMAC-2393]
- Es posible que se borren las credenciales de ciertos sitios web, sin permitir que los usuarios inicien sesión. [RFMAC-2394]
- Al iniciar Outlook Web App, se muestra una página en blanco. [RFMAC-2395]
- Al minimizar y maximizar aplicaciones integradas, es posible que la aplicación no se muestre correctamente. [RFMAC-2411]
- Es posible que los usuarios no puedan cargar archivos en Jira cuando se inicia como aplicación publicada. [RFMAC-2467]

Problemas resueltos en la versión 1903.1

- Puede que la aplicación Citrix Workspace para Mac se cierre inesperadamente al iniciar sesiones de escritorio.
- Es posible que algunas aplicaciones personalizadas no se inicien. [RFMAC-2081]
- Al mover la aplicación Bloc de notas, es posible que la aplicación se mueva al segundo plano cuando dos o más aplicaciones estén activas. [RFMAC-2107]
- Al intentar modificar un almacén de Citrix Workspace, aparece la interfaz de usuario de Citrix Files. [RFMAC-2111]
- Al hacer clic en el icono Dock después de iniciar una aplicación integrada antes de que la aplicación integrada esté lista, la sesión ya no será integrada. [RFMAC-2139]
- Después de desactivar el modo de suspensión de un MacBook, Citrix Workspace solicita la autenticación repetidamente. [RFMAC-2161]
- Después de volver a conectarse a una sesión de VDA integrada, es posible que los gráficos de la sesión estén distorsionados. [RFMAC-2176]
- Cuando se utiliza una distribución de teclado local y un teclado japonés, es posible que la eliminación de caracteres escritos no confirmados no funcione correctamente. [RFMAC-2287]

Problemas resueltos en la versión 1901

- Es posible que las aplicaciones no se inicien después de actualizar la aplicación Citrix Workspace para Mac. [RFMAC-2003]
- Es posible que la redirección USB de audio no funcione correctamente. [RFMAC-2043]
- No puede seleccionar menús desplegables en versiones integradas de Microsoft Outlook. [RFMAC-2079]
- Las sesiones pueden dejar de responder cuando se utilizan aplicaciones integradas. [RFMAC-2083]

- Las sesiones pueden dejar de responder al minimizar o maximizar las ventanas que abarcan varios monitores. [RFMAC-2103]

Problemas resueltos en la versión 1812

- Al leer el texto de ayuda en una aplicación de Microsoft Office, queda un rastro negro donde apareció el texto de ayuda. [RFMAC-1793]
- Las sesiones pueden aparecer borrosas cuando se utiliza una resolución Retina. [RFMAC-1944]
- Es posible que al usar el deslizamiento de tres dedos en un panel táctil en una sesión que se ejecuta en tres monitores no funcione correctamente. [RFMAC-1968]
- Puede que Citrix Viewer use la función de ahorro de energía App Nap cuando se ejecute en segundo plano. [RFMAC-1979]
- Al interrumpirse la conexión de red, es posible que la página de inicio de sesión tarde más de lo habitual en reaparecer una vez que se haya vuelto a conectar a la red. [RFMAC-2001]
- Al pulsar la tecla Eliminar, se puede eliminar más de un carácter. [RFMAC-2011]
- Puede que los VDA con EDT habilitado dejen de responder al reproducir vídeos de YouTube durante más de tres minutos. [RFMAC-2017]
- Si Citrix Receiver Launcher está registrado con Google Chrome, la actualización a la aplicación Citrix Workspace no permite el inicio de sesiones desde Chrome. [RFMAC-2020]
- Es posible que la directiva Usar códec de vídeo para compresión no funcione correctamente. [RFMAC-2021]

Problemas resueltos en la versión 1809

- Puede que las sesiones que se han reconectado no se mantengan conectadas. [RFMAC-1823]

Problemas resueltos en la versión 1808

- En los Mac de GPU duales, el cliente puede usar la GPU discreta con alimentación por batería en lugar de la GPU integrada más eficiente en el uso de la energía. [RFMAC-1439]
- Es posible que el cliente no se actualice correctamente cuando se instala con JamF. [RFMAC-1523]
- Es posible que los dispositivos USB no aparezcan en una sesión cuando intente usarlos para la redirección USB genérica. [RFMAC-1592]
- La comprobación de las actualizaciones del cliente puede fallar con un error de “Problema al comprobar actualizaciones”. [RFMAC-1589]
- Cuando se abre más de una ventana de una aplicación publicada, la activación de una ventana de aplicación publicada puede dar como resultado que una ventana de aplicación publicada diferente aparezca en primer plano. [RFMAC-1696]

Problemas conocidos

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

Beta de macOS Big Sur

- 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]

Optimización para Microsoft Teams (Tech Preview)

- Solo se pueden compartir aplicaciones de terceros (por ejemplo, Microsoft PowerPoint) cuando usted comparte 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]
- 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]
- 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]
- 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]

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.

Problemas conocidos en la versión 2005

- 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 en la versión 2002

- La aplicación Citrix Workspace para Mac ofrece la redirección de cámaras web solo en aplicaciones publicadas de 32 bits. Como consecuencia, no se ofrece la redirección de cámaras web en la aplicación Microsoft Teams publicada de 64 bits. [RFMAC-2199]
- La aplicación Citrix Workspace para Mac no admite pantallas de PPP elevados (Retina). Como consecuencia, es posible que el texto se vea borroso en esos dispositivos. [RFMAC-650]
- Es posible que no se pueda iniciar sesión en la aplicación Citrix Workspace desde macOS Catalina mediante tarjetas inteligentes PIV y que aparezca este mensaje de error: "No se pudo detectar la cuenta especificada". [CVADHELP-14155]

Problemas conocidos en la versión 2001

- Es posible que no se pueda iniciar sesión en la aplicación Citrix Workspace en macOS Catalina mediante tarjetas inteligentes PIV y que aparezca el siguiente mensaje de error: "No se pudo detectar la cuenta especificada". [CVADHELP-12609]
- Es posible que no se puedan iniciar sesiones en la aplicación Citrix Workspace desde macOS Catalina (10.15.2) mediante tarjetas inteligentes PIV y que aparezca este mensaje de error: "One or more root certificates is not valid" (Al menos uno de los certificados raíz no es válido). [RFMAC-3365]

Problemas conocidos en la versión 1912

No se han observado nuevos problemas en esta versión.

Problemas conocidos en 1910.2

- El inicio de sesión en la aplicación Citrix Workspace en macOS Catalina mediante tarjetas inteligentes PIV podría fallar. [RFMAC-2788]

Problemas conocidos en la versión 1910.1

- El inicio de sesión en la aplicación Citrix Workspace en macOS Catalina mediante tarjetas inteligentes PIV podría fallar. [RFMAC-2788]

Problemas conocidos en la versión 1910

- Al utilizar FaceTime en un MacBook Pro 2018 y versiones posteriores, es posible que los usuarios vean una barra verde en la parte inferior de la vista previa del vídeo. [RFMAC-2317]
- Es posible que no se puedan iniciar sesiones con una tarjeta inteligente a través de Citrix Gateway, tras lo cual aparece el mensaje de error "El homólogo SSL remoto envió una alerta de fallo de negociación". [RFMAC-2727]
- El inicio de sesión en la aplicación Citrix Workspace en macOS Catalina mediante tarjetas inteligentes PIV podría fallar. [RFMAC-2788]
- Cuando la autenticación SAML está habilitada, es posible que la pantalla de autenticación tarde en responder o directamente no responda. Como solución temporal, reinicie el dispositivo. [RFMAC-3047]
- Al denegar el permiso de automatización después de iniciar las aplicaciones suscritas, es posible que la aplicación Citrix Workspace para Mac deje de responder. Como solución temporal, vaya a **Preferencias del Sistema > Seguridad y privacidad > Privacidad > Automatización** y habilite permisos para Citrix Viewer.app, Citrix Workspace.app y todas las aplicaciones suscritas. [RFMAC-3048]

Problemas conocidos en la versión 1906

- Al utilizar FaceTime en un MacBook Pro 2018 y versiones posteriores, es posible que los usuarios vean una barra verde en la parte inferior de la vista previa del vídeo. [RFMAC-2317]

Problemas conocidos en la versión 1903.1

- Es posible que las sesiones de tarjetas inteligentes se desconecten de forma aleatoria. [RFMAC-1816]
- Al iniciar sesión, puede aparecer un error que indica que el servidor no se pudo encontrar. [RFMAC-2192]
- Al utilizar FaceTime en un MacBook Pro 2018 y versiones posteriores, es posible que los usuarios vean una barra verde en la parte inferior de la vista previa del vídeo. [RFMAC-2317]

Problemas conocidos en la versión 1901

- Es posible que las sesiones de tarjetas inteligentes se desconecten de forma aleatoria. [RFMAC-1816]

Problemas conocidos en la versión 1812

- Es posible que las sesiones de tarjetas inteligentes se desconecten de forma aleatoria. [RFMAC-1816]

- Es posible que la redirección USB de audio no funcione correctamente. [RFMAC-2043]

Problemas conocidos en la versión 1809

- Es posible que las sesiones de la aplicación y el escritorio no se inicien al usar la versión 12 de Safari. Como solución temporal, consulte el artículo CTX238286 de Knowledge Center. Después de aplicar la solución temporal, Safari solicita los permisos que los usuarios deben consentir cada vez que inicien sesiones.

Problemas conocidos en la versión 1808

- Cuando se produce un error con una aplicación que utiliza SaaS seguro, el error que aparece dentro del explorador no está localizado. [RFMAC-1836]

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

June 10, 2021

Sistemas operativos compatibles

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

- 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 la tabla de ciclos de vida de productos Citrix.

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:

- HTTP
- 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:**
>
> Si el certificado de la puerta de enlace remota no se puede verificar en la conexión (debido a que no se incluyó el certificado raíz en el almacén de claves local), se muestra un mensaje de advertencia sobre la presencia de un certificado que no es de confianza. Cuando un usuario decide 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 más información sobre esta tarea, consulte la documentación de Citrix Gateway. Para obtener más información sobre cómo instalar y vincular un certificado intermedio con una CA principal en un dispositivo Citrix Gateway, consulte How to Install and Link Intermediate Certificate with Primary CA on Citrix Gateway (Cómo instalar y vincular un certificado intermedio con una CA principal en 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 presentes en el servidor o 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 “Certificado raíz de ejemplo”. Si la aplicación Citrix Workspace para Mac no confía en “Certificado raíz de ejemplo”, 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 docu-

> mentación de la entidad de certificación para determinar qué certificado raíz debe usarse. Tenga en cuenta que 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 uno que se valida correctamente y también es de confianza (por ejemplo, "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 usan un certificado intermedio con firmas cruzadas. Esto está pensado para casos en los 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, habrá 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”
- “Certificado intermedio con firmas cruzadas de ejemplo” [no se recomienda]

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					

	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)
Token de seguridad				Sí*	Sí*
Dos factores (dominio con token de seguridad)				Sí*	Sí*
SMS				Sí*	Sí*
Tarjeta inteligente	Sí	Sí		Sí*	Sí
Certificado de usuario				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

April 12, 2021

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 ello, descargue el archivo desde el sitio web de Citrix, en Descargas.

Para instalar la aplicación Citrix Workspace para Mac:

1. Descargue el archivo DMG para la versión de la aplicación Citrix Workspace para Mac que desea instalar desde el sitio web de Citrix y abra ese archivo.
2. En la página Introducción, haga clic en **Continuar**.
3. En la página **Licencia**, haga clic en **Continuar**.
4. Haga clic en **Aceptar** para aceptar los términos del contrato de licencia.
5. En la página **Tipo de instalación**, haga clic en **Instalar**.
6. En la página **Agregar cuenta**, seleccione **Agregar cuenta** y haga clic en **Continuar**.
7. 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.

Actualizaciones

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. También puede hacer clic con el botón secundario en el icono de la aplicación Citrix Workspace y hacer clic en **Comprobar actualizaciones** para averiguar si hay revisiones o actualizaciones disponibles.

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

Configuración

June 18, 2021

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.

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`
- `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 la 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 más información sobre el estado 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

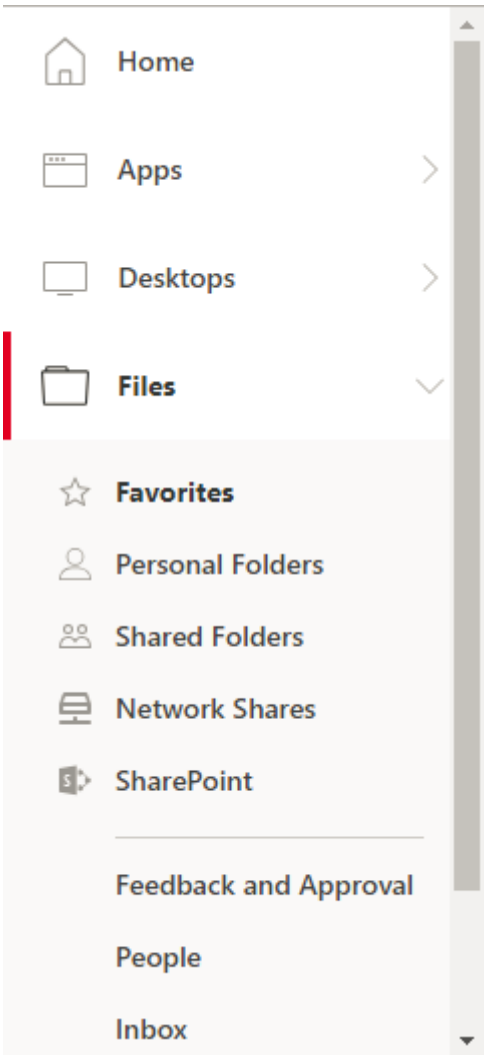
Citrix Content Collaboration le permite intercambiar documentos de forma fácil y segura, enviar documentos grandes por correo electrónico, manejar de forma segura transferencias de documentos a terceros y acceder a un espacio de colaboración.

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:**
>
> La integración de Citrix Content Collaboration en la aplicación Citrix Workspace no está disponible en Windows Server 2012 ni en Windows Server 2016. Esto se debe a una opción de seguridad del 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. Por ejemplo, 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**
>
> En los entornos donde es necesario hacer una separación de seguridad entre el servidor y el dispositivo de usuario, Citrix recomienda dar instrucciones 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

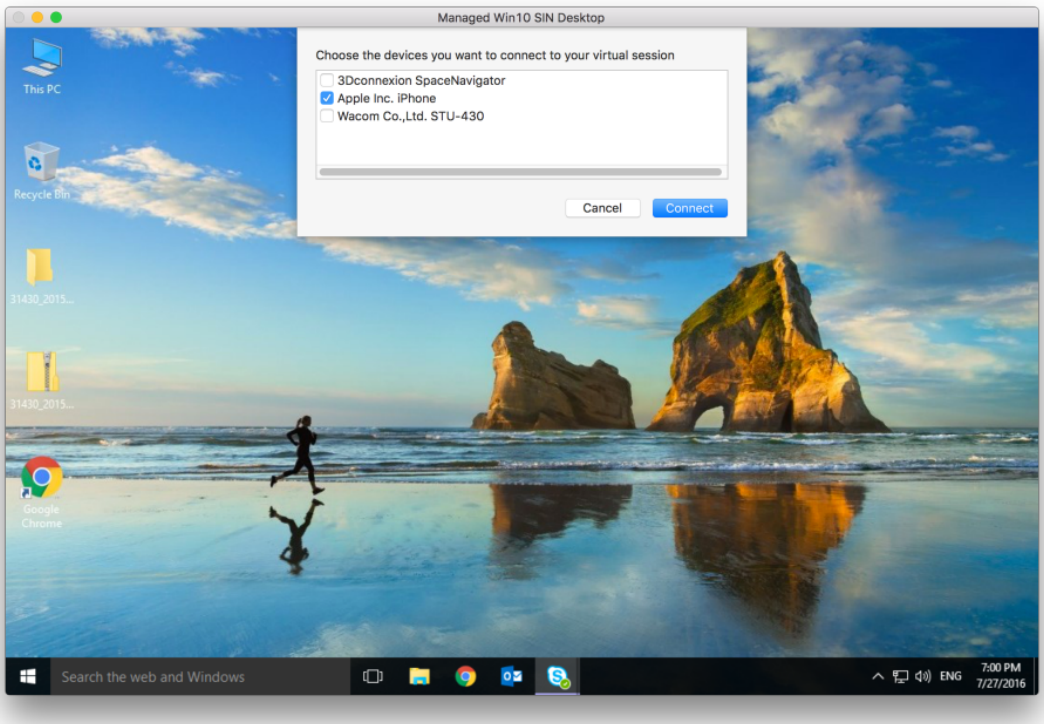
unos auriculares. El producto también admite la redirección de USB genérico de dispositivos USB 3.0 conectados a puertos USB 2.0.

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. Si esto supone un problema, utilice el canal virtual de USB genérico.

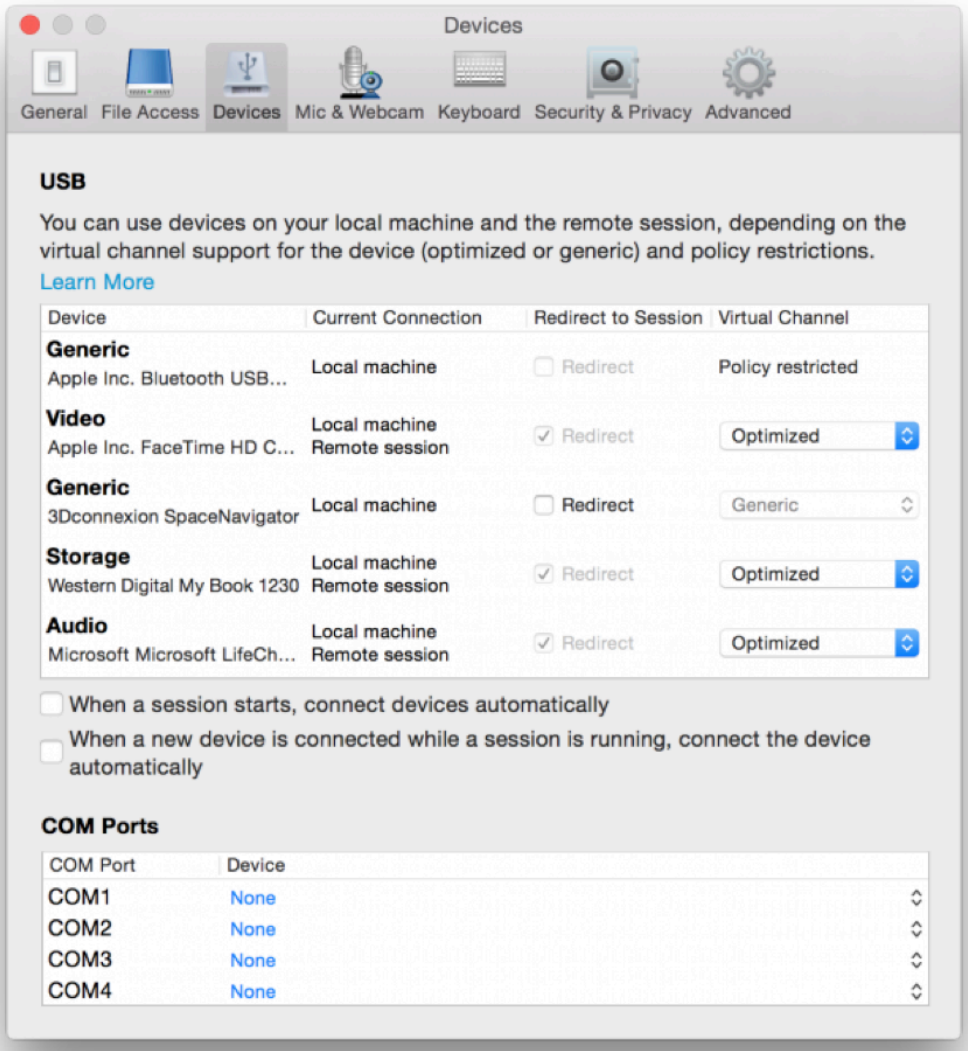
Algunos dispositivos no se redireccionan de manera predeterminada y solo están disponibles en la sesión local. Por ejemplo, no sería adecuado redirigir una tarjeta de interfaz de red que está conectada directamente por USB interno.

Para usar la redirección de USB:

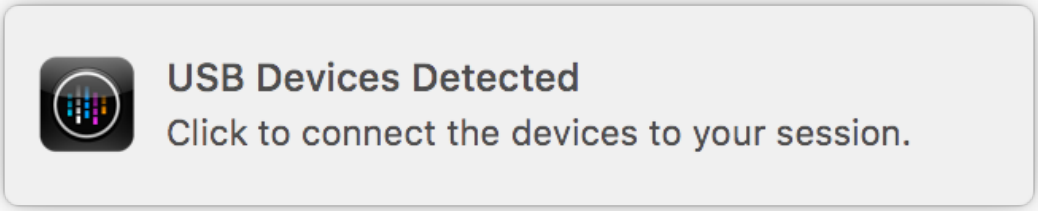
1. Conecte el dispositivo USB al dispositivo donde está instalada la aplicación Citrix Workspace para Mac.
2. Se le pedirá que seleccione los dispositivos USB disponibles en el sistema local.



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.

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. El usuario sigue teniendo acceso a la presentación en pantalla durante la interrupción y puede reanudar la interacción con la aplicación después de restablecerse la conexión de red. 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.
> - Si la fiabilidad de la sesión está 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 **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**
>
> A medida que prolonga el tiempo que una sesión se mantiene abierta, es posible que un usuario se distraiga y se aleje de su dispositivo. Esto puede dejar la sesión accesible para usuarios no autorizados.

Las conexiones entrantes con la función 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.

Si no desea que los usuarios se reconecten con sesiones interrumpidas sin tener que repetir la autenticación, use la función Reconexión automática de clientes. 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 trascurrido 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.

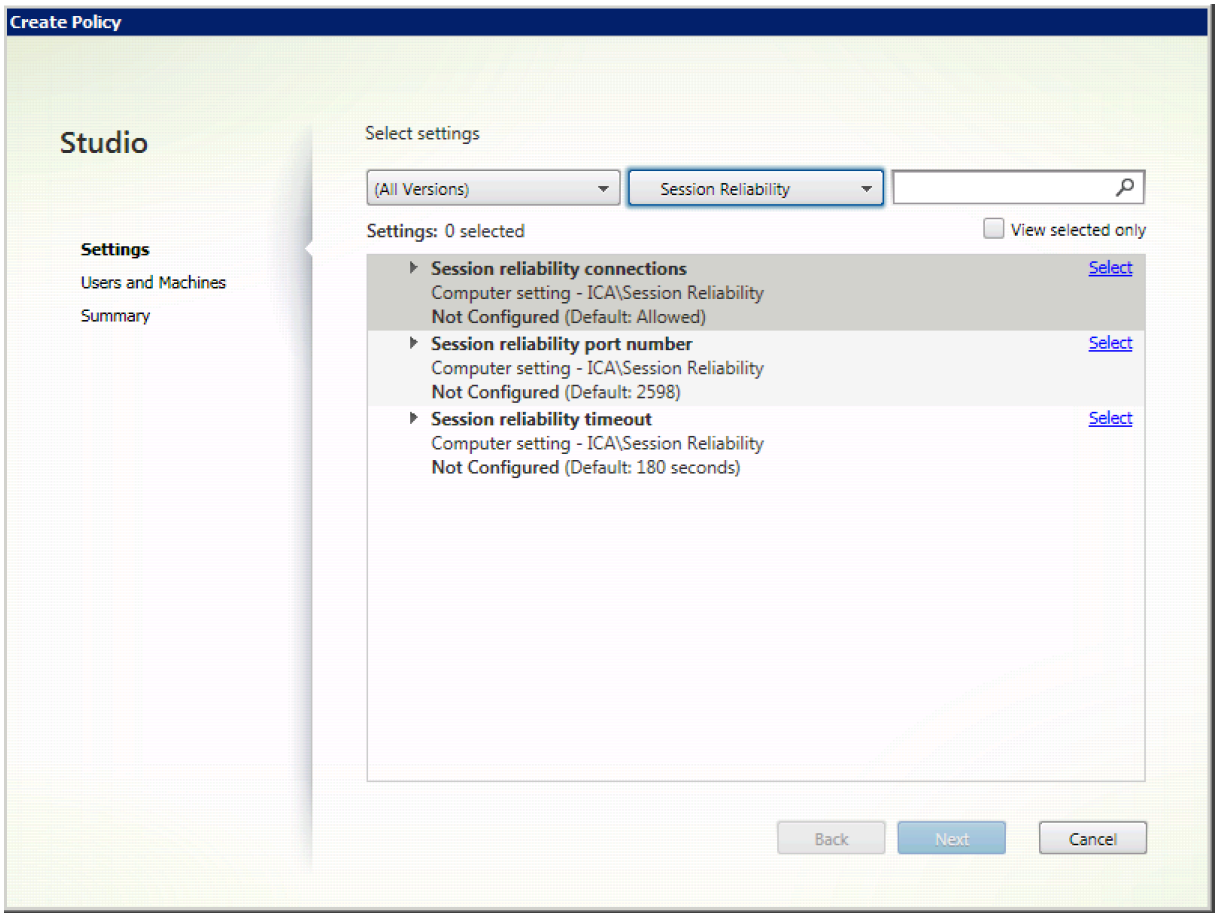
> **Nota**
>
> De forma predeterminada, la fiabilidad de sesión se habilita en el servidor. Para inhabilitar esta función, configure la directiva administrada por el servidor.

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:

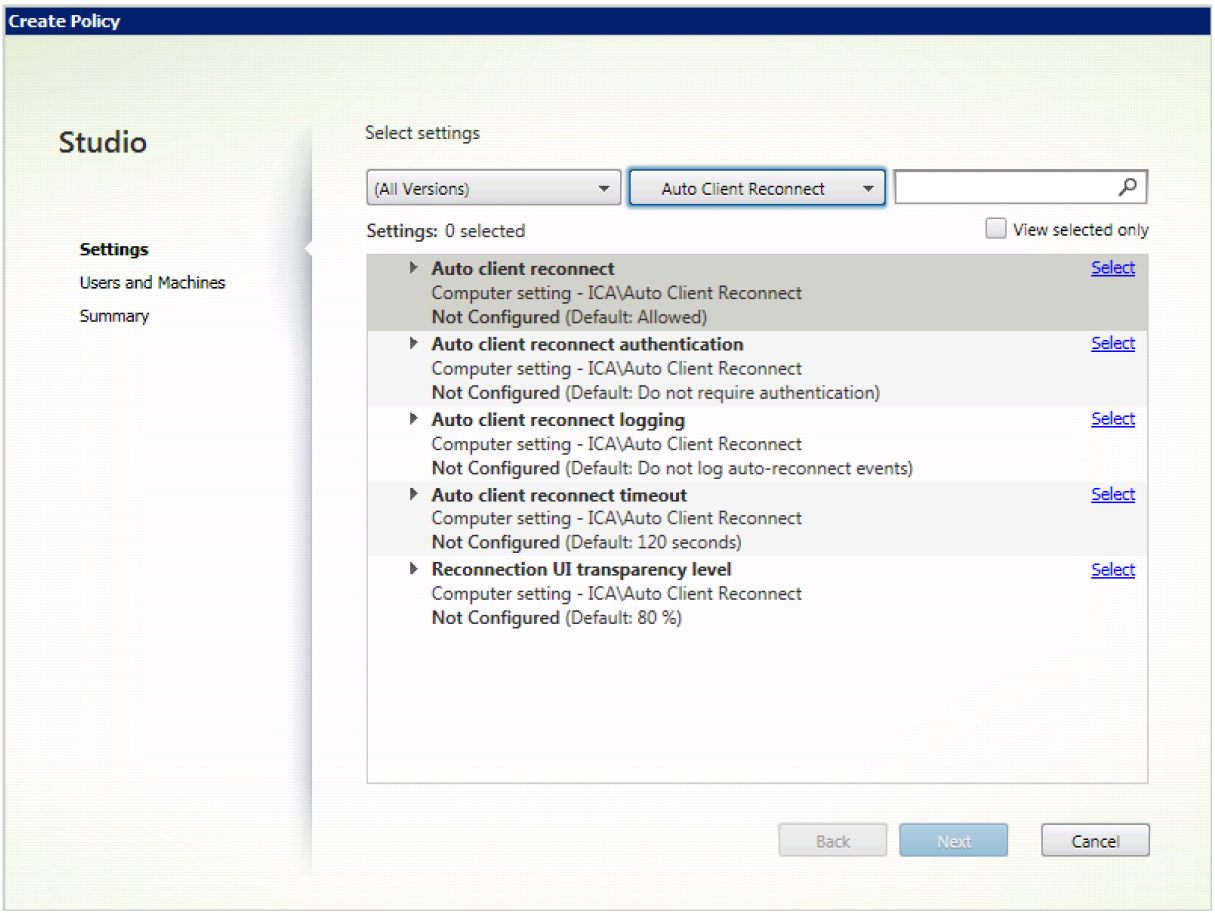
1. Abra Citrix Studio.
2. Abra la directiva **Tiempo de espera de fiabilidad de la sesión**.
3. Cambie el valor del tiempo de espera.
4. Haga clic en **Aceptar**.

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 tiene un valor de 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. Para solucionar este problema, las tecnologías mejoradas de Citrix de fiabilidad de la sesión y reconexión automática están presentes en esta versión de la aplicación Citrix Workspace para Mac.

La reconexión automática de clientes, junto con la fiabilidad de la sesión, permiten a los usuarios reconectarse automáticamente con sus sesiones de la aplicación Citrix Workspace para Mac después de recuperarse de una interrupción en la red. Estas funciones se habilitan mediante directivas en Citrix Studio y se pueden utilizar para mejorar sustancialmente la experiencia del 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 AutoClientReconnect. 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).

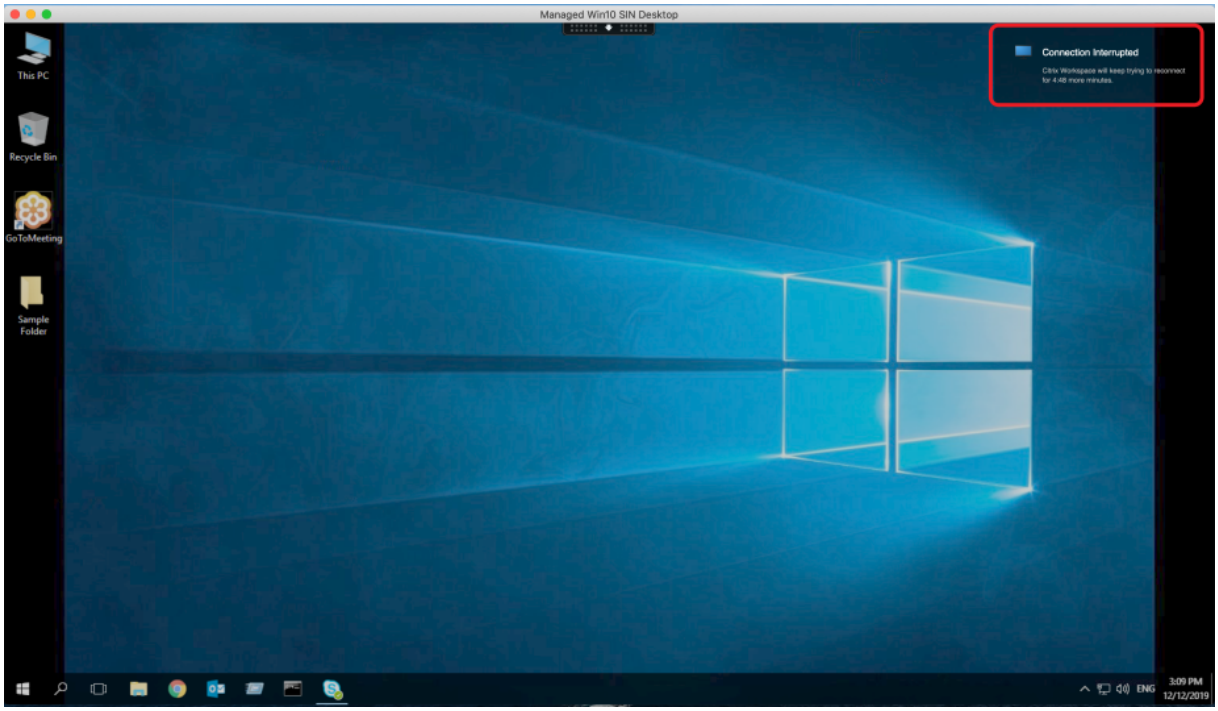
Parámetro	Ejemplo	Valor predeterminado
SessionReliabilityTTL	SessionReliabilityTTL=120	180

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.

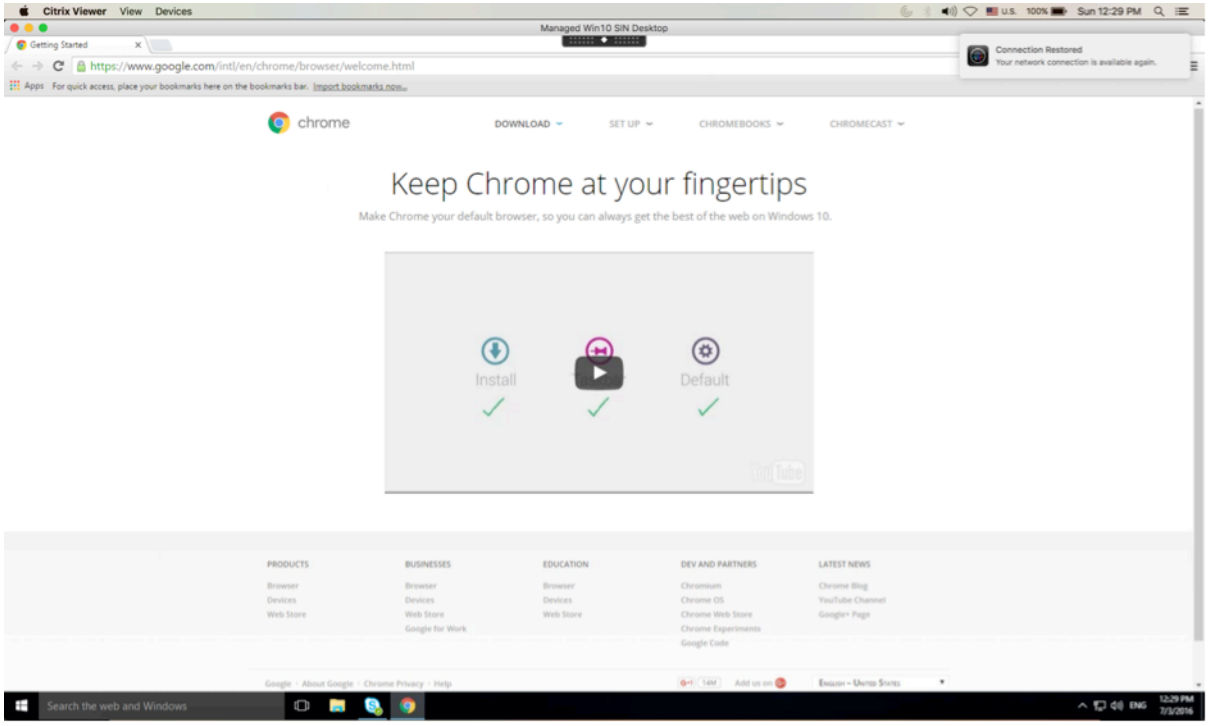
De forma predeterminada, la notificación de cuenta atrás de reconexión comienza en 5 minutos. El valor de este temporizador representa los valores predeterminados combinados de cada temporizador (el de la reconexión automática del cliente y el de la fiabilidad de la sesión), que son 2 y 3 minutos, respectivamente. 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:



- 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.

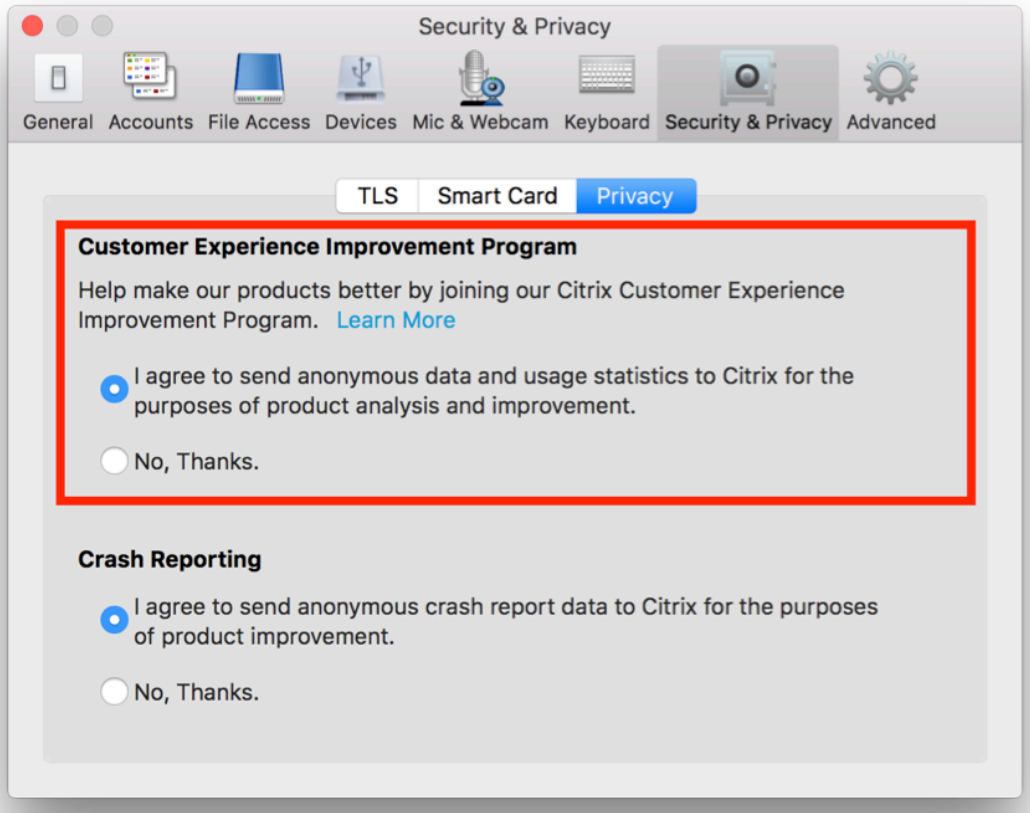
Información adicional

Citrix gestionará sus datos de acuerdo con los términos de su contrato con Citrix y los protegerá como se especifica en el anexo de seguridad de Citrix Services, 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 Google gestiona los datos recopilados para Google Analytics.

Puede desactivar el envío de datos de CEIP a Citrix y a Google Analytics. Para hacerlo:

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 quieran. 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. Para ello, debe incluir descripciones útiles en 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 a todos los usuarios de un almacén a una aplicación, agregue la cadena KEYWORDS:Auto a la descripción que proporcionará cuando publique la aplicación en Citrix Virtual Apps. Cuando los usuarios inicien sesión en el almacén, la aplicación se suministrará 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 ello, agregue la cadena KEYWORDS:Featured a la descripción de la aplicación.

Para obtener más información, consulte la documentación del 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 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

Esto determina que la aplicación Citrix Workspace para Mac puede detectar si las actualizaciones están disponibles.

Valores válidos:

- Auto: Con esta opción, recibirá notificaciones cuando existan actualizaciones disponibles.
- Manual: Con esta opción, no recibirá notificaciones cuando existan actualizaciones disponibles. Los usuarios deben buscar manualmente las actualizaciones. Para ello, deberán seleccionar **Comprobar actualizaciones**.
- Disabled: Con esta opción, se inhabilitan 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 siempre tiene la opción de recibir un recordatorio más tarde cuando una actualización esté 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 entregar a los usuarios las actualizaciones disponibles.
- Fast: Las actualizaciones disponibles se aplican 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 aplican 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 (por ejemplo, al ejecutar aplicaciones como administrador) no se pueden sincronizar con la distribución de 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 RDP se implementa como una aplicación y el usuario está trabajando en una sesión RDP, no es posible cambiar la distribución del teclado con los accesos directos Alt + Mayús. Para solucionar este problema, los usuarios pueden usar la barra de idioma en 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
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 Workspace**/, 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 que se ejecutan en 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 del Citrix Ready Workspace Hub.

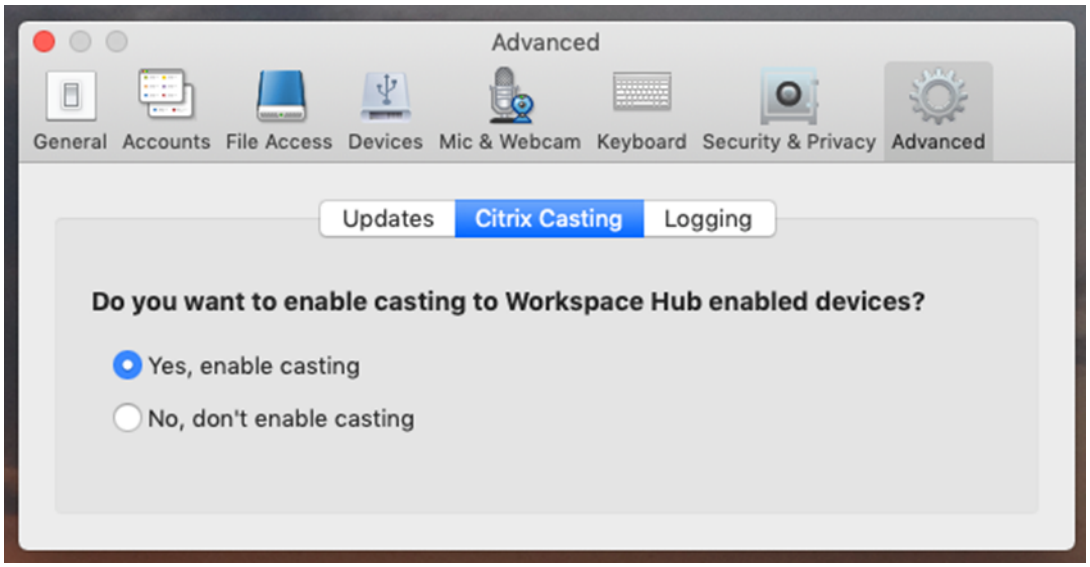
Requisitos previos

- 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.

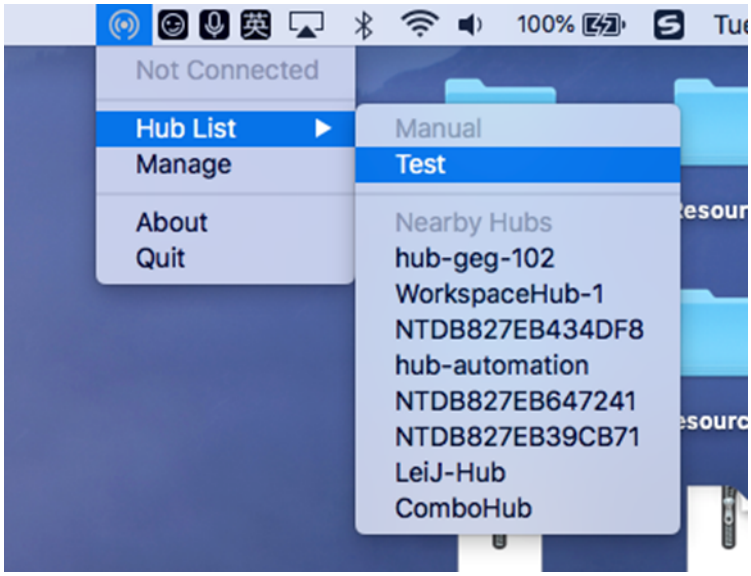
> **Nota:**
>
> Una vez habilitado, Citrix Casting se inicia automáticamente con la aplicación Citrix Workspace

> 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**.

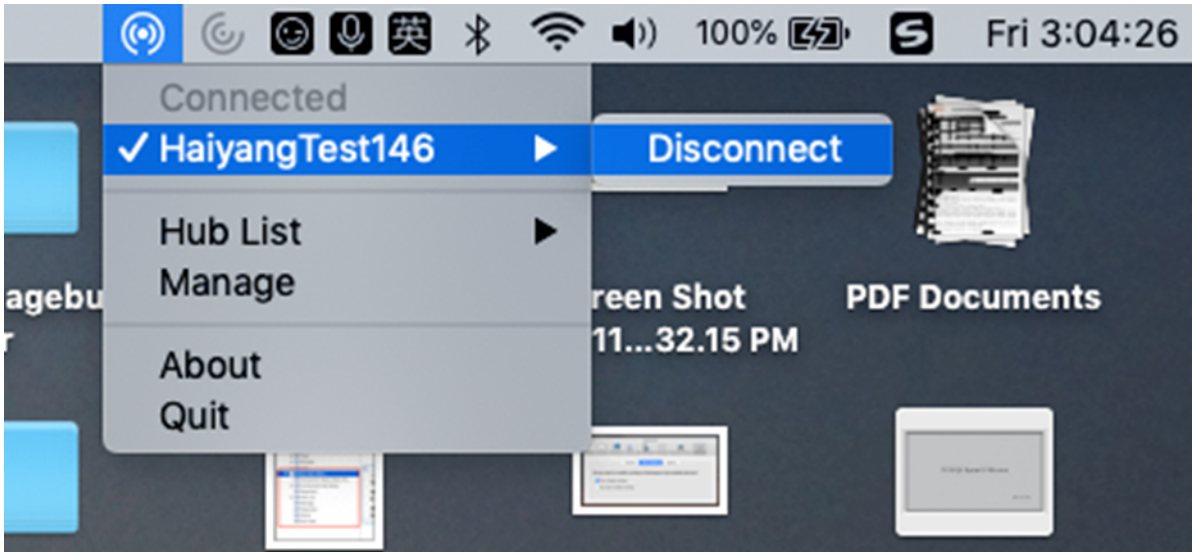
> **Nota:**
>
> Actualmente, solo se admite el modo **Duplicar**. **Duplicar** es la única opción disponible en la columna **Modo de pantalla**.

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 los micrófonos conectados al dispositivo de usuario en las sesiones, seleccione una de las siguientes opciones en la ficha Micrófono y cámara web en la **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" 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" 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
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 para Mac 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 son aquellas que crean entradas de texto e incluyen todas las letras, números y signos de puntuación. Las teclas especiales son aquellas que 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

Tecla o combinación de teclas de Windows	Equivalentes de Mac
Ctrl+Alt+Suprimir	Control-Opción-Fn-Comando-Suprimir; seleccione Teclado > Enviar Ctrl-Alt-Sup
Eliminar	Suprimir; seleccione Teclado > Enviar clave > Suprimir; Fn-Retroceso (Fn-Suprimir en algunos teclados para Estados Unidos)
Fin	Fin; Fn-Flecha derecha
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 las siguientes 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. Seleccione Desktop Viewer y haga clic en la flecha hacia abajo.
2. Seleccione la opción **Ventana**.
3. Arrastre la pantalla Citrix Virtual Desktops entre los monitores. Asegúrese de que aproximadamente la mitad de la pantalla esté presente en cada monitor.
4. En la barra de herramientas de Citrix Virtual Desktops, seleccione **Pantalla completa**.

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. Para salir del modo de pantalla completa y pasar al modo de ventana, se puede seguir alguno de estos métodos:
  - En OS X 10.10, haga clic en el botón de ventana verde en la barra de menú desplegable.

  - En OS X 10.9, haga clic en el botón de menú azul en la barra de menú desplegable.
  - Para todas las versiones de OS X, seleccione **Salir de pantalla completa** en el menú **Visualización** de la barra de menú desplegable.
- El comportamiento de arrastre de la barra de herramientas se ha actualizado para admitir el arrastre entre ventanas de 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. Esto permite, 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 cierra sesión en un dispositivo de usuario ubicado en la sala de emergencias de un hospital y, a continuación, inicia sesión en una estación de trabajo del laboratorio de rayos X del hospital. 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 cuando el usuario inicia sesión en el dispositivo de usuario ubicado en el laboratorio de rayos X.

Para configurar los parámetros de control del espacio de trabajo

1. Haga clic en el icono con la flecha hacia abajo 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 un servidor se configura para permitir la asignación de unidades del cliente, los usuarios

pueden acceder a los archivos almacenados localmente, trabajar con esos archivos durante las sesiones y guardarlos nuevamente 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 icono con la flecha hacia abajo 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.

Autenticarse

August 14, 2020

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 tarjetas inteligentes, como Microsoft Outlook y Microsoft Office. Estas aplicaciones permiten a los usuarios firmar o cifrar digitalmente documentos disponibles en sesiones de aplicaciones o escritorios virtuales.

- 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

May 24, 2021

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 desea utilizar la aplicación Citrix Workspace para Mac a través de un firewall que asigna la dirección IP de red interna del servidor a una dirección de Internet externa (es decir, 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 asistencia 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 sobre el modo Relay de traspaso, 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 Citrix Secure Web Gateway.

- El número de puerto del servidor 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 Citrix 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 validado, 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, no se admiten ni TLS_ECDHE_RSA_WITH_AES_2 ni TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384. Citrix Gateway debe configurarse para utilizar 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.

Según los procedimientos y las directivas de la empresa, tal vez quiera instalar el certificado raíz en cada dispositivo de usuario 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. Esto inicia automáticamente la aplicación Acceso a llaves.
2. En el cuadro de diálogo Añadir certificados, elija una de las siguientes opciones en el menú emergente Llavero:
    - 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. Los clientes compatibles con TLS y todas las aplicaciones que utilicen TLS podrán usar el certificado raíz.

Acerca de las directivas de TLS

Esta sección proporciona información sobre cómo configurar directivas de seguridad para sesiones ICA sobre TLS en la aplicación Citrix Workspace para Mac. 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 pueden administrar de otras maneras, por ejemplo, cuando los dispositivos están controlados por OS X Server o alguna 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:

- **Ninguno**. 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. Este parámetro 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. Esta función mejora la autenticación criptográfica del servidor Citrix y mejora la seguridad global de las conexiones SSL/TLS entre clientes y servidores. Este parámetro controla cómo se trata una entidad de certificación raíz durante un intento de 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 que un administrador revoque certificados de seguridad (no válidos después de su fecha de caducidad) en el caso de exista un riesgo criptográfico para la clave privada, o simplemente si ha habido un cambio inesperado 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 hace una comprobación de listas de revocación de certificados, incluida la entidad de certificación (CA) 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 arriba.

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

<value>: El valor del parámetro. Si el valor es una matriz (array) y se están especificando varios valores, éstos deben ir separados por espacios.

```
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

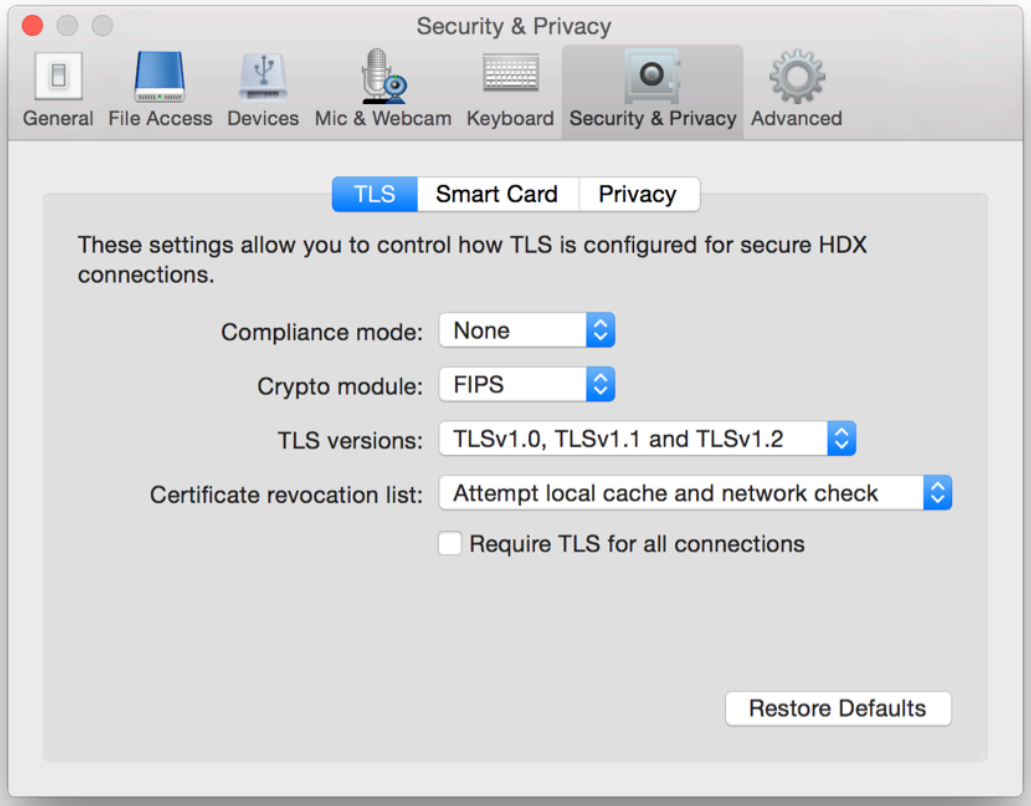
En la versión 12.3 de Citrix Receiver para Mac, se han introducido numerosas mejoras, que incluyen lo siguiente:

- 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 para configurar la seguridad son más sencillos y accesibles desde la interfaz de usuario, lo que mejora la experiencia del usuario, ya que crea un método directo para definir las preferencias relacionadas con la seguridad.
- ver conexiones TLS. Puede verificar las conexiones realizadas a servidores que utilizan una versión específica de TLS, el algoritmo de cifrado utilizado para la conexión, el modo, el tamaño de la clave y el estado 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