Aplicación Citrix Workspace para iOS

Contents

Acerca de esta versión

January 15, 2021

Novedades en la versión 21.1.0

Compatibilidad con las versiones para iOS

La aplicación Citrix Workspace 21.1.0 para iOS es la versión más reciente compatible con la versión 10.x de iOS.

Novedades en la versión 20.12.0

En esta versión se resolvieron una serie de problemas para mejorar la estabilidad y el rendimiento general.

Novedades en la versión 20.11.0

Vista web mejorada con controles nativos para aplicaciones SaaS

Con esta versión, puede tener una vista web mejorada con controles nativos para aplicaciones SaaS. Esta mejora permite:

- Ver la URL de las aplicaciones.
- Ver la información de seguridad de las aplicaciones.
- Compartir las aplicaciones.

Además, ahora puede deslizar el dedo hacia la izquierda y hacia la derecha sobre las aplicaciones para avanzar y retroceder, respectivamente.

Novedades en la versión 20.10.5

Disponibilidad de teclas especiales

En esta versión se admiten las siguientes combinaciones de teclas en teclados externos de iOS:

- Windows + R
- Windows + D
- Windows + E
- Windows + L
- Windows + M

- Windows + S
- Windows + CTRL + S
- Windows + T
- Windows + U
- Windows + Número
- Windows + Flecha arriba
- Windows + Flecha abajo
- Windows + Flecha izquierda
- Windows + Flecha derecha
- Windows + X
- Windows + K
- CTRL + ESC

Novedades en la versión 20.10.0

En esta versión se resolvieron una serie de problemas para mejorar la estabilidad y el rendimiento general.

Novedades en la versión 20.9.5

En esta versión se resolvieron una serie de problemas para mejorar la estabilidad y el rendimiento general.

Novedades en la versión 20.9.0

Uso compartido externo de páginas web

Con esta versión, puede compartir con otros usuarios las páginas web que abra desde la aplicación Citrix Workspace para iOS. Puede hacer lo siguiente:

- Copiar enlaces desde una vista web
- Abrir páginas web directamente en Safari
- Enviar enlaces directamente a usuarios o aplicaciones

Para ello, toque el icono **...** de la parte superior derecha de la vista web o mantenga pulsado cualquier enlace dentro de la vista web y toque la opción que necesite.

Novedades en la versión 20.8.1

En esta versión se resolvieron una serie de problemas para mejorar la estabilidad y el rendimiento general.

Novedades en la versión 20.8.0

En esta versión se resolvieron una serie de problemas para mejorar la estabilidad y el rendimiento general.

Novedades en la versión 20.7.6

En esta versión se resolvieron una serie de problemas para mejorar la estabilidad y el rendimiento general.

Novedades en la versión 20.7.5

En esta versión se resolvieron una serie de problemas para mejorar la estabilidad y el rendimiento general.

Novedades en la versión 20.7.0

Compatibilidad con monitores externos y la barra de herramientas

La función Monitor externo y la barra de herramientas ya están disponibles. Esta versión también corrige errores relacionados con esta función.

Compatibilidad con mouse y paneles táctiles genéricos

Con esta versión, puede utilizar un mouse o un panel táctil para hacer clic con el botón secundario, desplazarse hacia arriba y hacia abajo, y pasar el cursor por sesiones HDX. Las acciones son similares a las de Citrix X1 Mouse. El estilo del cursor del mouse local cambia para que coincida con el del cursor remoto.

> **Notas:**
>
> - Esta función está disponible a partir de iPadOS 13.4.
> - Esta función no está disponible en iPhones.

Limitación:

Si tiene un monitor externo conectado mientras está en una sesión, el cursor del mouse genérico permanece en el dispositivo nativo debido a una limitación de iOS.

Compatibilidad con autenticación de varios factores (nFactor)

La autenticación de varios factores mejora la seguridad de las aplicaciones porque requiere que los usuarios proporcionen varias pruebas de identidad para obtener acceso. La autenticación de varios factores hace que el administrador pueda configurar los pasos de autenticación y los formularios de recopilación de credenciales asociados.

La aplicación Citrix Workspace nativa puede admitir este protocolo a partir de la funcionalidad de formularios de inicio de sesión ya implementada para StoreFront. La página de inicio de sesión web de los servidores virtuales de Citrix Gateway y Traffic Manager también utiliza este protocolo.

Para obtener más información, consulte Autenticación SAML y Autenticación de varios factores (nFactor).

Limitación:

Con la autenticación nFactor habilitada, no se puede utilizar autenticación biométrica como Touch ID y Face ID.

Disponibilidad de teclas especiales

Esta versión permite el uso de las siguientes teclas individuales en un teclado externo a partir de iOS 13.4:

- RePág
- AvPág
- Inicio
- Finalizar
- F1
- F2
- F3
- F4
- F5
- F6
- F7
- F8
- F9
- F10
- F11
- F12

Novedades en la versión 20.6.0

Compatibilidad con monitores externos y la barra de herramientas Vista previa de la función

A partir de esta versión, puede utilizar Citrix X1 Mouse para utilizar la barra de herramientas en un monitor externo. Ahora puede mover la muesca de la barra de herramientas horizontalmente mientras esta está cerrada. Al conectar el dispositivo iOS al monitor externo, la aplicación Citrix Workspace detecta automáticamente la resolución de la pantalla de dicho monitor. Puede utilizar el botón **Pantalla** de la barra de herramientas para seleccionar una resolución de pantalla concreta. Puede acceder a la opción **Pantalla** sin tener que agregar una cuenta o iniciar sesión primero.

Novedades en la versión 20.5.0

En esta versión se resolvieron una serie de problemas para mejorar la estabilidad y el rendimiento general.

Novedades en la versión 20.4.5

En esta versión se resolvieron una serie de problemas para mejorar la estabilidad y el rendimiento general.

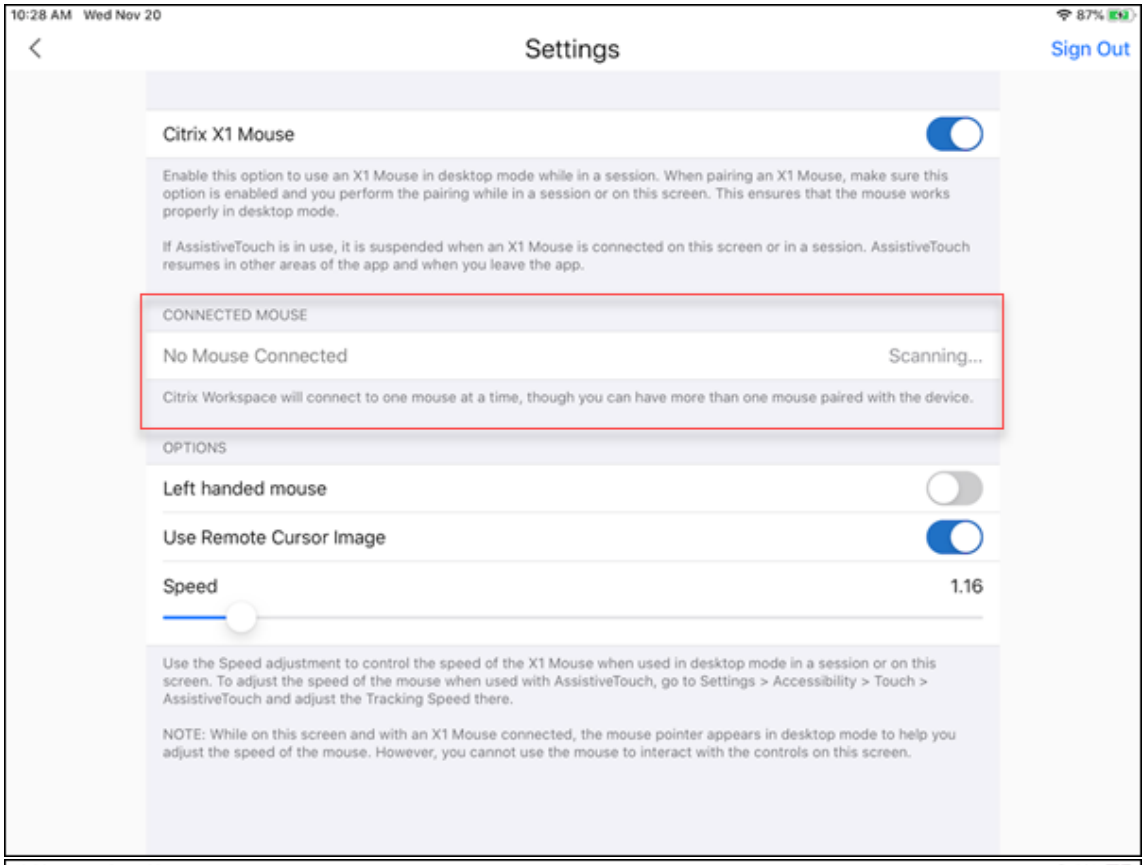
Novedades en la versión 20.4.0

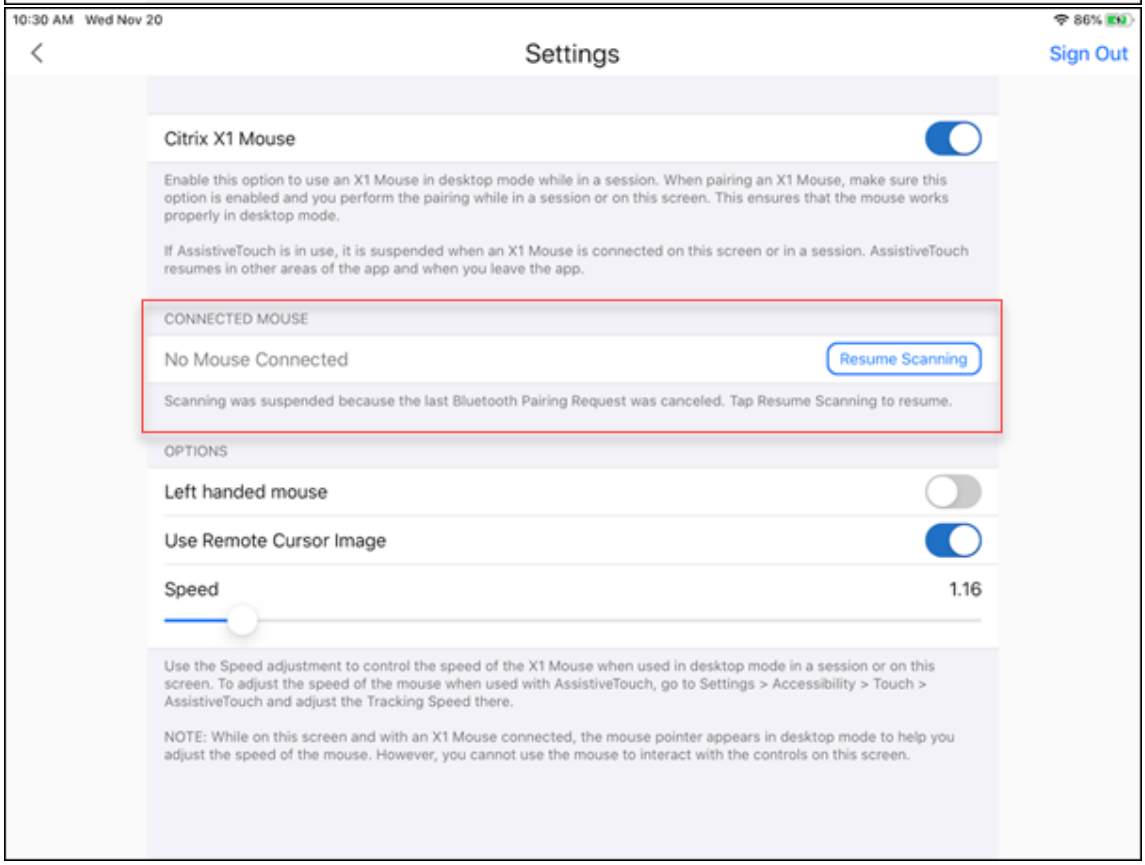
> **Nota:**
>
> A partir de junio de 2020, la aplicación Citrix Workspace deja de ser compatible con la versión 11.x del sistema operativo iOS. Como alternativa, actualice la versión de su sistema operativo iOS a la versión 12 o a una posterior.

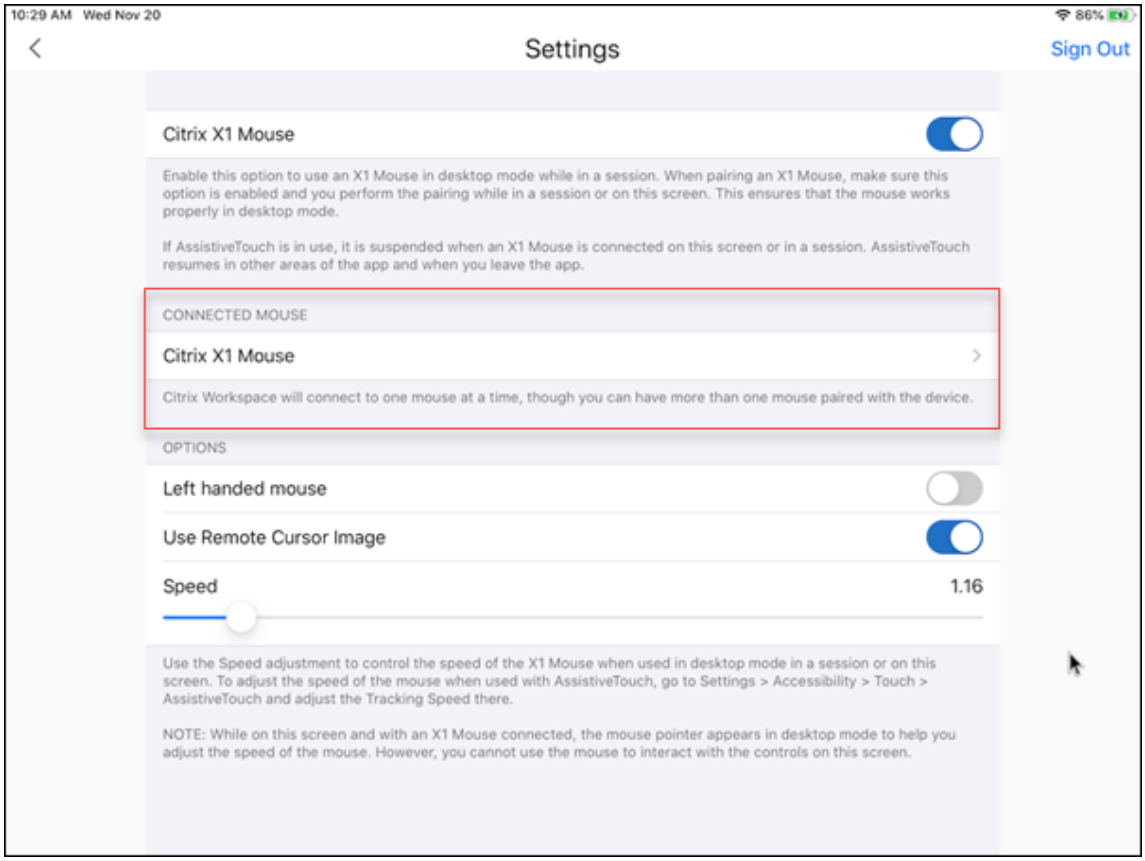
Estado de conexión y emparejamiento de dispositivos Citrix X1 Mouse

Esta función le permite tener más control sobre el proceso de emparejamiento de dispositivos Citrix X1 Mouse. En la pantalla **Ajustes**, puede:

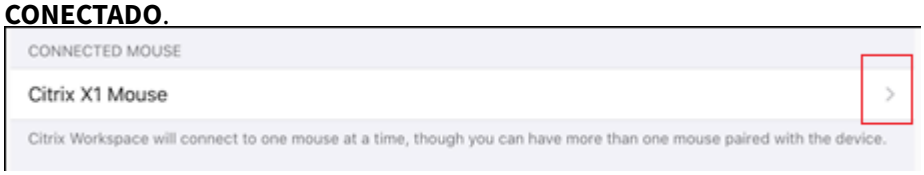
- Emparejar el dispositivo Citrix X1 Mouse. También puede emparejar un dispositivo X1 Mouse cuando se halle en una sesión.
- Ver el estado de la conexión.







- Consultar las propiedades del dispositivo Citrix X1 Mouse, como, por ejemplo, **Nombre**, **UUID**, **Revisión del firmware** y **Nivel de batería**. Para ello, toque la entrada Citrix X1 Mouse en **MOUSE CONECTADO**.



Propiedades del mouse conectado:

![propiedades de AssistiveTouch] (/en-us/citrix-workspace-app-for-ios/media/assistivetouch-properties.png)

AssistiveTouch

Con la función AssistiveTouch habilitada en iOS 13 o en versiones posteriores, puede ver el cursor de AssistiveTouch si cambia entre el modo de mouse de escritorio y el modo AssistiveTouch.

> **Nota:**
>
> En el modo de ratón de escritorio, aparece el cursor con forma de puntero. En el modo AssistiveTouch, aparece el cursor redondo.

El cursor de AssistiveTouch aparece:

- Al abandonar una sesión
- Al ir a la pantalla Selector de app de iOS
- Al ir a la pantalla de inicio de iOS u otra aplicación

El modo de escritorio se reanuda cuando vuelve a la aplicación Citrix Workspace y cuando se halla en una sesión.

Novedades en la versión 20.3.0

En esta versión se resolvieron una serie de problemas para mejorar la estabilidad y el rendimiento general.

Novedades en la versión 20.2.2

En esta versión se resolvieron una serie de problemas para mejorar la estabilidad y el rendimiento general.

Novedades en la versión 20.2.0

En esta versión se resolvieron una serie de problemas para mejorar la estabilidad y el rendimiento general.

Novedades en 20.1.5

En esta versión se resolvieron una serie de problemas para mejorar la estabilidad y el rendimiento general.

Novedades en la versión 20.1.0

En esta versión se resolvieron una serie de problemas para mejorar la estabilidad y el rendimiento general.

Problemas resueltos

Problemas resueltos en la versión 21.1.0

En los iPad con iOS 13 o una versión posterior, es posible que las aplicaciones SaaS se abran en el explorador seguro incluso cuando el parámetro **Aplicar directiva en dispositivos móviles** no esté seleccionada en la consola de administración. [CVADHELP-16596]

Problemas resueltos en versiones anteriores

Problemas resueltos en la versión 20.12.0

En esta versión se resolvieron una serie de problemas para mejorar la estabilidad y el rendimiento general.

Problemas resueltos en la versión 20.11.0

En esta versión se resolvieron una serie de problemas para mejorar la estabilidad y el rendimiento general.

Problemas resueltos en la versión 20.10.5

En iPads y iPhones con una nueva instalación de la aplicación Citrix Workspace para iOS 20.7.0 y versiones posteriores, puede que los certificados de cliente no se importen. Como resultado, aparece el siguiente mensaje de error.

```
Certificate cannot be imported. Error when importing into the key chain
because the certificate is not in P12 format.
```

[CVADHELP-15685]

Problemas resueltos en la versión 20.10.0

En una configuración en la nube, es posible que las aplicaciones iniciadas recientemente desde Citrix Workspace para iOS no se carguen en el widget Hoy ni en iPhone ni en iPad. [RFIOS-5528]

Problemas resueltos en la versión 20.9.5

En esta versión se resolvieron una serie de problemas para mejorar la estabilidad y el rendimiento general.

Problemas resueltos en la versión 20.9.0

- En implementaciones en la nube, es posible que no se pueda iniciar sesión en la aplicación Citrix Workspace para iOS cuando Azure Active Directory o Google Identity Provider se utilizan como proveedores de identidades. [CVADHELP-14845]
- Al usar la aplicación Citrix Workspace para iOS en un iPad en el modo horizontal, la barra de herramientas de la página **Parámetros > Administrar cuenta > Agregar nueva cuenta > Configuración manual** se desplaza hacia la derecha y oculta el enlace **Guardar**. [CVADHELP-15376]
- En los escritorios publicados, es posible que el puntero táctil desaparezca de manera inesperada al cerrar o minimizar una sesión y volver a ella. [CVADHELP-15354]

Problemas resueltos en la versión 20.8.1

En esta versión se resolvieron una serie de problemas para mejorar la estabilidad y el rendimiento general.

Problemas resueltos en la versión 20.8.0

- En un dispositivo iOS, la combinación de teclas CTRL+MAYÚS no funciona de la manera prevista. El problema se produce al conectar un teclado externo al dispositivo. [CVADHELP-15048]
- Cuando se inicia una aplicación publicada, la pantalla de Desktop Viewer aparece en negro y la sesión se desconecta. [CVADHELP-14628]

Problemas resueltos en la versión 20.7.6

- Durante una sesión, no es posible introducir caracteres con un teclado externo, a no ser que se toque la opción **Teclado** en la barra de herramientas de la sesión. El problema ocurre en dispositivos iOS 12.x. [CVADHELP-14779]
- Con un teclado externo conectado a un dispositivo iOS 12.x, las teclas extendidas no aparecen al tocar en la opción **Teclado** de la barra de herramientas de la sesión. [CVADHELP-14674]

Problemas resueltos en la versión 20.7.5

- Los intentos de conectarse a un almacén oculto pueden fallar después de actualizar la aplicación Citrix Workspace a la versión 20.5.0.5. [CVADHELP-14998]

Problemas resueltos en la versión 20.7.0

En esta versión se resolvieron una serie de problemas para mejorar la estabilidad y el rendimiento general.

Problemas resueltos en la versión 20.6.0

- Antes, al agregar una cuenta de almacén web, la aplicación Citrix Workspace para iOS ignoraba los errores de certificado. A partir de esta versión, aparece un mensaje de error apropiado al agregar un almacén web o una cuenta de interfaz web con un certificado no válido. [RFIOS-5403]

Problemas resueltos en la versión 20.5.0

- Se produce un error al iniciar aplicaciones dentro de la aplicación Citrix Workspace con el siguiente error:
  "CAMAuthManErrorNoSuitableLogonProtocol"

El problema se produce debido a una API incorrecta. [RFIOS-5530]

Problemas resueltos en la versión 20.4.5

- En un teclado que no sea inglés, al introducir las credenciales en la página **Iniciar sesión**, el contenido del campo **Contraseña** aparece en inglés. [CVADHELP-14068]

Problemas resueltos en la versión 20.4.0

- Es posible que la acción asignada a un gesto de doble pulsación no funcione como se esperaba. El problema se produce cuando un toque adicional de la aplicación Citrix Workspace realiza una acción diferente. La acción de doble pulsación funciona correctamente cuando se utiliza el mouse Citrix X1 o un mouse en pantalla. [RFIOS-4814]
- El teclado en pantalla aparece en cada toque incluso después de desacoplarlo. [RFIOS-5267]
- Al cerrar la sesión de una cuenta en la nube desde **Ajustes** > **Almacén** > **Cerrar sesión**, es posible que el proceso de cierre de sesión no funcione de la forma esperada. El problema se produce de forma intermitente en iPhones. [RFIOS-5197]
- Después de cambiar un DNS, el inicio de una sesión podría fallar con un error de conexión. Este problema se produce debido a una resolución IP obsoleta en la caché. [RFIOS-5358]

Problemas resueltos en la versión 20.3.0

- En una configuración en la nube, al abrir la aplicación Citrix Workspace, el recuento de insignias de la aplicación no se borra. [RFIOS-5194]

Problemas resueltos en la versión 20.2.2

- Single Sign-On no es compatible con Citrix Files. [RFIOS-5564]

Problemas resueltos en la versión 20.2.0

- Si pulsa el botón Atrás en la sesión de Citrix Gateway, es posible que se cierre la sesión y se le devuelva a la página de inicio de sesión. El problema se produce cuando se accede a la aplicación Citrix Workspace a través de la Interfaz Web (WI). [RFIOS-5059]
- Es posible que las modificaciones aplicadas a un grupo de entrega no se sincronicen con el almacén. Como resultado, la lista de aplicaciones no se actualiza. [RFIOS-5103]
- Puede que el puntero del mouse Citrix X1 desaparezca inesperadamente. El problema se produce si deja la aplicación Citrix Workspace con una sesión en ejecución o con la pantalla de configuración del mouse abierta y, a continuación, vuelve a la aplicación Citrix Workspace. [RFIOS-5349]

Problemas resueltos en 20.1.5

- Los intentos de importar un token de software al hacer clic en un archivo `.sdtid` podrían fallar. El problema ocurre en iOS 13.3 y iPadOS 13.3. [RFIOS-5236]
- La aplicación Citrix Workspace se cierra inesperadamente después del 1 de enero de 2020 cuando se utiliza la cámara en una sesión publicada. El problema no se produce cuando se establece manualmente la fecha en 2019. [RFIOS-5208]
- En una configuración de nube, es posible que observe un recuento incorrecto de insignias. [RFIOS-5195]

Problemas resueltos en la versión 20.1.0

- Es posible que no se pueda iniciar escritorios publicados mediante un VDA alojados en la nube. El problema se produce cuando los VDA se inician apagados. [RFIOS-5027]
- Es posible que no se puedan agregar cuentas mediante la detección de cuentas basada en correo electrónico y que aparezca el siguiente mensaje de error:

  ```
  Cannot Add Account. Workspace cannot find the server for this domain.
  If you received a URL from your IT, you can enter that instead of your
  email.
  ```

  El problema se produce al actualizar la versión 1910.5 a la 1911. [RFIOS-5052]

Problemas conocidos

Problemas conocidos en la versión 21.1.0

No se han observado nuevos problemas conocidos en esta versión.

Problemas conocidos en versiones anteriores

Problemas conocidos en la versión 20.12.0

No se han observado nuevos problemas conocidos en esta versión.

Problemas conocidos en la versión 20.11.0

No se han observado nuevos problemas conocidos en esta versión.

Problemas conocidos en la versión 20.10.5

No se han observado nuevos problemas conocidos en esta versión.

Problemas conocidos en la versión 20.10.0

No se han observado nuevos problemas conocidos en esta versión.

Problemas conocidos en la versión 20.9.5

No se han observado nuevos problemas conocidos en esta versión.

Problemas conocidos en la versión 20.9.0

- En una configuración en la nube, es posible que las aplicaciones iniciadas recientemente desde Citrix Workspace para iOS no se carguen en el widget Hoy en iPhone ni en iPad. [RFIOS-5528]
- Es posible que, de manera intermitente, no se puedan abrir archivos ICA descargados desde el explorador web Safari. Este problema se produce en la aplicación Citrix Workspace para iOS en dispositivos con iOS 14. Pruebe estas dos soluciones temporales:
  - Espere un poco antes de abrir el archivo descargado (aunque aparezca el icono de descarga completa)
  - Vaya a **Ajustes > Descargas de Safari**. Seleccione **En mi iPad** para guardar los archivos descargados.

[RFIOS-6599]

Problemas conocidos en la versión 20.8.1

No se han observado nuevos problemas conocidos en esta versión.

Problemas conocidos en la versión 20.8.0

No se han observado nuevos problemas conocidos en esta versión.

Problemas conocidos en la versión 20.7.6

No se han observado nuevos problemas conocidos en esta versión.

Problemas conocidos en la versión 20.7.5

No se han observado nuevos problemas conocidos en esta versión.

Problemas conocidos en la versión 20.6.0

No se han observado nuevos problemas conocidos en esta versión.

Problemas conocidos en la versión 20.5.0

No se han observado nuevos problemas conocidos en esta versión.

Problemas conocidos en la versión 20.4.5

No se han observado nuevos problemas conocidos en esta versión.

Problemas conocidos en la versión 20.4.0

No se han observado nuevos problemas conocidos en esta versión.

Problemas conocidos en la versión 20.3.0

No se han observado nuevos problemas conocidos en esta versión.

Problemas conocidos en la versión 20.2.2

No se han observado nuevos problemas conocidos en esta versión.

Problemas conocidos en la versión 20.2.0

- Al cerrar la sesión de una cuenta en la nube desde **Ajustes** > **Almacén** > **Cerrar sesión**, es posible que el proceso de cierre de sesión no funcione de la forma esperada. El problema se produce de forma intermitente en iPhones. Como solución temporal, reinicie la aplicación Citrix Workspace. [RFIOS-5197]
- Cuando se modifica y se guarda la configuración del **Almacén** y, a continuación, se cancelan las modificaciones cancelando la autenticación, es posible que la cuenta de Workspace se elimine de la aplicación. El problema se produce en una configuración de nube. [RFIOS-5433]
- En una configuración en la nube, al modificar y guardar la configuración de la cuenta, la aplicación Citrix Workspace puede dejar de responder de forma intermitente. Como solución temporal, reinicie la aplicación Citrix Workspace. [RFIOS-5379]

Problemas conocidos en 20.1.5

- En una configuración en la nube, al abrir la aplicación Citrix Workspace, el recuento de insignias de la aplicación no se borra. [RFIOS-5194]
- Al cerrar la sesión de una cuenta en la nube desde **Ajustes** > **Almacén** > **Cerrar sesión**, es posible que el proceso de cierre de sesión no funcione de la forma esperada. El problema se produce de forma intermitente en iPhones. Como solución temporal, reinicie la aplicación Citrix Workspace. [RFIOS-5197]

Problemas conocidos en 20.1.0

- En una configuración de nube, es posible que observe un recuento incorrecto de insignias. [RFIOS-5194]
- En dispositivos iOS 13.3, es posible que observe un recuento incorrecto de insignias. [RFIOS-5204]
- La opción “Probar la demo” no está disponible. [RFIOS-4902]

Limitaciones

- No se pueden iniciar aplicaciones si se toca el archivo ICA en el gestor de descargas al utilizar el explorador web Safari. Para garantizar que las aplicaciones se inicien correctamente desde Safari, compruebe que la versión más reciente de la aplicación Citrix Workspace o Citrix Receiver para iOS (pero no ambas) esté presente en el dispositivo. [RFIOS-5502]

Vista previa de la función

Las vistas previas de funciones están disponibles para que los clientes las usen en sus entornos de producción limitados o en entornos que no son de producción, y para darles la oportunidad de compartir comentarios. Citrix no acepta casos de asistencia para vistas previas de funciones, pero agradece comentarios para mejorarlas. Citrix puede o no actuar a partir de los comentarios en función de su gravedad e importancia.

Requisitos previos para la instalación

October 20, 2020

Requisitos del sistema y compatibilidad

Requisitos de dispositivo

- La versión 2009 de la aplicación Citrix Workspace para iOS y versiones posteriores son compatibles con iOS 14 y iPadOS 14.
- La versión 1909 de la aplicación Citrix Workspace para iOS y versiones posteriores son compatibles con iOS 13 y iPadOS.
- La versión 1808 de la aplicación de Citrix Workspace para iOS y versiones posteriores son compatibles con iOS 12.
- Esta actualización de software ha sido validada en los dispositivos siguientes:
  - Modelos iPhone 7x, modelos iPhone 8x y solo el modelo iPhone X.

  - Todos los modelos de iPad (incluido iPad Pro) con la excepción del iPad 1 y el iPad 2, que no son compatibles.
- Funcionalidad de presentación en pantallas externas
  - iPhone: Lo compatible con iOS.
  - iPad: Lo compatible con iOS (no usa toda la pantalla).

Requisitos del servidor

Asegúrese de que instala las revisiones hotfix más recientes en los servidores.

- Para conexiones con aplicaciones y escritorios virtuales, la aplicación Citrix Workspace para iOS es compatible con Citrix StoreFront y la Interfaz Web.

  StoreFront:

  - StoreFront 3.6 o versiones posteriores (recomendado). La aplicación Citrix Workspace para iOS ha sido validada con la versión más reciente de StoreFront; entre las versiones anteriores compatibles están StoreFront 2.6 y posteriores.

    Ofrece acceso directo a almacenes de StoreFront. La aplicación Citrix Workspace para iOS también es compatible con versiones anteriores de StoreFront.

    > **Nota:**
    >
    > Con XenApp y XenDesktop 7.8, Citrix introdujo el canal virtual Framehawk y 3D Pro. Esta funcionalidad se amplió a la aplicación Citrix Workspace para iOS.

  - StoreFront configurado con Workspace para sitios web

    Da acceso a los almacenes de StoreFront a través de un explorador web Safari. Los usuarios deben abrir manualmente el archivo ICA con el explorador web. Para conocer las limitaciones de esta implementación, consulte la documentación de StoreFront.

  Interfaz Web:

  - Interfaz Web 5.4 con sitios de Interfaz Web
  - Interfaz Web 5.4 con sitios de XenApp y XenDesktop
  - Interfaz Web en Citrix Gateway (solo acceso basado en explorador web con Safari)

    Debe habilitar las directivas de reescritura suministradas por Citrix Gateway.

- **Citrix Virtual Apps and Desktops**, **XenApp** y **XenDesktop** (cualquiera de los siguientes productos):
  - Citrix Virtual Apps and Desktops 7 1808 o versiones posteriores.
  - Citrix XenDesktop 7.x o versiones posteriores
  - Citrix XenApp 7.5 o versiones posteriores

Conexiones, certificados y autenticación

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

	Workspace para Web con exploradores	Sitio de servicios StoreFront (nativo)	Sitio de XenApp y XenDesktop 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*	Sí*
PassThrough de dominio	Sí	Sí	Sí		
Token de seguridad				Sí*	Sí*
Autenticación de dos factores (dominio con token de seguridad)				Sí*	Sí*
SMS				Sí*	No
Tarjeta inteligente		Sí		Sí*	Sí*
Certificado de usuario				Sí (plug-in de Citrix Gateway)	Sí (plug-in de Citrix Gateway)

* Disponible solo para sitios de Workspace para Web y para implementaciones que incluyen Citrix Gateway, con o sin el plug-in asociado en el dispositivo.

Para conexiones con la Interfaz Web 5.4, la aplicación Citrix Workspace para iOS admite los siguientes métodos de autenticación:

> **Nota:**
>
> La Interfaz Web usa el término “Explícita” para la autenticación con dominio y token de seguri-

> dad.

	Interfaz Web (exploradores web)	Sitio de XenDesktop y XenApp de Interfaz Web	De Citrix Gateway a la Interfaz Web (explorador web)	Citrix Gateway en el sitio de XenApp y XenDesktop de Interfaz Web
Anónimo	Sí			
Dominio	Sí	Sí	Sí*	
PassThrough de dominio	Sí			
Token de seguridad			Sí*	
Autenticación de dos factores (dominio con token de seguridad)			Sí*	
SMS			Sí*	
Tarjeta inteligente				
Certificado de usuario			Sí (requiere el plug-in de Citrix Gateway)	

Certificados

Certificados privados (autofirmados)

Cuando se ha instalado un certificado privado en la puerta de enlace remota, se debe disponer de un certificado raíz para la entidad de certificación de la empresa en el dispositivo con el fin de poder acceder correctamente a los recursos Citrix mediante la aplicación Citrix Workspace para iOS.

> **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. Si un usuario elige ignorar la

> advertencia y continuar con la conexión, se mostrará la lista de aplicaciones, pero no se podrán iniciar.

Certificado instalado de forma manual

En iOS 10.3 y versiones posteriores, SSL (Capa de sockets seguros) no confía automáticamente en un certificado que esté incluido en un perfil e instalado de forma manual. Para confiar en perfiles de certificados instalados de forma manual en iOS:

1. Asegúrese de haber instalado el perfil de certificado en el dispositivo.
2. Vaya a **Ajustes** > **General** > **Información** > **Ajustes de confianza de los certificados**.

   Cada raíz que se haya instalado mediante un perfil aparecerá en **Confiar en los certificados raíz**.
3. Puede habilitar o inhabilitar la confianza para cada certificado raíz.

Importación de certificados raíz en dispositivos iPhone y iPad

Obtenga el certificado raíz de la entidad de certificación y envíelo por correo electrónico a una cuenta de correo electrónico 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 iOS admite certificados comodín.

Certificados intermedios y Citrix Gateway

Cuando la cadena de certificados incluye un certificado intermedio, es necesario añadir ese certificado intermedio al certificado de servidor de Citrix Gateway (o Access Gateway). Además, para instalaciones de Access Gateway, consulte el artículo de Knowledge Center CTX114146 correspondiente a la edición que esté usando.

La autenticación con RSA SecurID es compatible con las configuraciones de Secure Gateway (mediante la Interfaz Web solamente) y todas las configuraciones de Access Gateway admitidas.

La aplicación Citrix Workspace para iOS admite todos los métodos de autenticación compatibles con Access Gateway.

Directiva de validación conjunta de certificados de servidor

Las versiones de la aplicación Citrix Workspace para iOS presentan una directiva más estricta para validar los certificados de servidor.

> **Importante**
>
> Antes de instalar la aplicación Citrix Workspace para iOS, 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 iOS 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 iOS 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 fallen las conexiones de la aplicación Citrix Workspace para iOS.

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 iOS:

- Certificado de servidor - ejemplo
- Certificado intermedio - ejemplo
- Certificado raíz - ejemplo

A continuación, la aplicación Citrix Workspace para iOS comprobará que todos los certificados son válidos. La aplicación Citrix Workspace para iOS comprobará también que ya confía en **Certificado raíz de ejemplo**. Si la aplicación Citrix Workspace para iOS 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 o GTE CyberTrust Global Root
- DigiCert Baltimore Root o Baltimore CyberTrust Root

Estos certificados 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, fallarán las conexiones de la aplicación Citrix Workspace para iOS en esos dispositivos de usuario. Consulte la documentación 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.

La aplicación Citrix Workspace para iOS usará esos dos certificados. Luego, buscará un certificado raíz en el dispositivo del usuario. Si encuentra uno que se valida correctamente y también es de confianza (por ejemplo, **Certificado raíz - ejemplo**), la conexión se realiza correctamente. De lo contrario, la conexión falla.

Tenga en cuenta que esta configuración proporciona el certificado intermedio que necesita la aplicación Citrix Workspace para iOS, pero también permite que la aplicación Citrix Workspace para iOS elija cualquier certificado raíz válido y de confianza.

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

- Certificado de servidor - ejemplo
- Certificado intermedio - ejemplo
- Certificado raíz incorrecto

Un explorador web podría ignorar el certificado raíz incorrecto. No obstante, la aplicación Citrix Workspace para iOS no ignorará el certificado raíz incorrecto y la conexión fallará.

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):

- Certificado de servidor - ejemplo
- Certificado intermedio 1 - ejemplo
- Certificado intermedio 2 - ejemplo

> **Importante**
>
> Algunas entidades de certificación usan un certificado intermedio con firmas cruzadas. Este tipo

> de certificado está pensado para situaciones en que hay más de un certificado raíz: un certificado raíz anterior se usa 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:

- Certificado de servidor - ejemplo
- Certificado intermedio - ejemplo

No configure la puerta de enlace para que use el certificado intermedio con firmas cruzadas, porque la aplicación Citrix Workspace para iOS seleccionará el certificado raíz anterior:

- Certificado de servidor - ejemplo
- Certificado intermedio - ejemplo
- Certificado intermedio con firmas cruzadas - ejemplo [no recomendado]

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

- Certificado de servidor - ejemplo

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

Instalación, actualización

August 17, 2020

Actualizaciones

Para actualizar la aplicación Citrix Workspace a la versión más reciente, realice cualquiera de los siguientes pasos:

- Descargue la aplicación Citrix Workspace de la página Descargas de Citrix e instale la aplicación para actualizar Citrix Receiver a la aplicación Citrix Workspace.
- Actualice la versión de la aplicación Citrix Workspace mediante el almacén de aplicaciones.

Para obtener información detallada sobre las funciones disponibles en la aplicación Citrix Workspace para iOS, consulte la tabla de funciones de la aplicación Citrix Workspace.

Introducción

October 20, 2020

Configurar

La aplicación Citrix Workspace para iOS admite la configuración de la Interfaz Web para la implementación de Citrix Virtual Apps. Hay dos tipos de sitios de Interfaz Web: sitios de XenApp y XenDesktop y sitios de Citrix Virtual Apps and Desktops. Los sitios de la Interfaz Web permiten a los dispositivos cliente conectarse con la comunidad de servidores. La autenticación entre la aplicación Citrix Workspace para iOS y el sitio de la Interfaz Web se puede gestionar mediante una variedad de soluciones, incluido Citrix Secure Web Gateway.

Además, se puede configurar StoreFront para proporcionar servicios de autenticación y entrega de recursos para la aplicación Citrix Workspace para iOS, lo que permite crear almacenes empresariales para la entrega de escritorios, aplicaciones y otros recursos para los usuarios.

Para obtener más información sobre cómo configurar las conexiones, incluidos vídeos, blogs y foros de asistencia, consulte http://community.citrix.com.

Para que los usuarios puedan acceder a las aplicaciones alojadas en la implementación de Citrix Virtual Apps and Desktops, antes hay que configurar los componentes siguientes en el entorno como se describe a continuación.

- Cuando publique aplicaciones en comunidades o sitios, tenga en cuenta las siguientes opciones para mejorar la experiencia de los usuarios que acceden a esas aplicaciones a través de almacenes de StoreFront.
  - Asegúrese de incluir descripciones significativas para las aplicaciones publicadas, dado que estas descripciones estarán visibles para los usuarios de la aplicación Citrix Workspace para iOS.

  - Puede destacar ciertas aplicaciones publicadas para los usuarios de los dispositivos móviles, incluyéndolas en la lista de Destacadas de la aplicación Citrix Workspace para iOS. Para rellenar esta lista en la aplicación Citrix Workspace para iOS, modifique las propiedades de las aplicaciones publicadas en los servidores y agregue la cadena de texto KEYWORDS:Featured al valor del campo Descripción de la aplicación.
  - Para habilitar el modo de ajuste de pantalla que ajusta la aplicación al tamaño de la pantalla de los dispositivos móviles, modifique las propiedades de las aplicaciones publicadas en los servidores y agregue la cadena de texto KEYWORDS:mobile en el valor del campo Descripción de la aplicación. Esta palabra clave también activa la función de desplazamiento automático para la aplicación.
  - 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 aprovisionará automáticamente sin que los usuarios tengan que suscribirse de forma manual a la aplicación.

- Si la Interfaz Web de la implementación de Citrix Virtual Apps and Desktops no dispone de un sitio web o un sitio de Citrix Virtual Apps and Desktops, cree uno. El nombre del sitio y la forma de crearlo depende de la versión de la Interfaz Web instalada. Para obtener instrucciones sobre cómo crear uno de estos sitios, consulte el tema “Creación de sitios” para su versión de la Interfaz Web.

Configuración manual

En general, cuando la aplicación Citrix Workspace para iOS se conecta con Citrix Gateway, intenta encontrar un sitio de XenApp y XenDesktop o un sitio web de Citrix Virtual Apps después de la autenticación. Si no se detecta ningún sitio, la aplicación Citrix Workspace para iOS muestra un error. Para evitar esta situación, puede configurar manualmente una cuenta de modo que la aplicación Citrix Workspace para iOS pueda conectar con Citrix Gateway.

1. Toque el icono Cuentas en la parte superior derecha; a continuación, en la pantalla Cuentas, toque el signo +. Aparecerá la pantalla Nueva cuenta.
2. En la parte inferior izquierda de la pantalla, toque el icono a la izquierda de Opciones y luego en Configuración manual. Aparecerán unos campos adicionales en la pantalla.
3. En el campo Dirección, introduzca la dirección URL segura del sitio o Citrix Gateway al que quiere conectarse (por ejemplo, `agee.mycompany.com`).
4. Seleccione alguna de estas opciones de conexión. Los demás campos de la pantalla cambiarán según lo que seleccione.
   - Interfaz Web: Seleccione si la aplicación Citrix Workspace para iOS mostrará un sitio web de Citrix Virtual Apps, similar a un explorador web. Esto se conoce como vista web.
   - Servicios XenApp: Esta opción permite a la aplicación Citrix Workspace para iOS encon-

trar un sitio de XenApp y XenDesktop concreto que no tenga configurada la autenticación mediante Citrix Gateway. En las opciones adicionales que aparecerán en la pantalla, introduzca las credenciales de inicio de sesión para el sitio.
  - <FQDN de StoreFront>: Si hay varios almacenes, se presenta una lista al usuario para que elija la que quiere agregar.
  - <FQDN de StoreFront>/citrix/<Nombre de almacén>: Esto agrega el almacén de StoreFront <Nombre de almacén>.
  - <FQDN de StoreFront>/citrix/PnAgent/config.xml: Esto agrega el antiguo almacén predeterminado de PNAgent.
  - <FQDN de StoreFront>/citrix/<Nombre de almacén>/PnAgent/config.xml: Esto agrega el antiguo almacén PNAgent asociado a <Nombre de almacén>.
- Citrix Gateway: Esta opción permite a la aplicación Citrix Workspace para iOS conectar con un sitio de XenApp y XenDesktop mediante un dispositivo Citrix Gateway concreto. En las opciones adicionales de esta pantalla, seleccione la edición del servidor y sus credenciales de inicio de sesión, y si requiere un token de seguridad para la autenticación.

5. Para el certificado de seguridad, use el parámetro del campo Ignorar advertencias de certificados para determinar si quiere conectar con el servidor, aunque este tenga un certificado no válido, autofirmado o caducado. El valor predeterminado es NO.
   Importante: Si decide habilitar esta opción, compruebe que se conecta al servidor correcto. Citrix recomienda encarecidamente que todos los servidores tengan un certificado válido para proteger a los dispositivos de usuario contra posibles ataques a la seguridad. Un servidor seguro usa un certificado SSL emitido por una entidad de certificación. Citrix no admite certificados autofirmados y no recomienda ignorar la seguridad de certificados.
6. Toque Guardar.
7. Introduzca su nombre de usuario y su contraseña (o token, si seleccionó la autenticación de dos factores), y toque Inicio de sesión. Aparecerá la pantalla de la aplicación Citrix Workspace para iOS, desde la cual puede acceder a sus escritorios, así como agregar y abrir aplicaciones.

StoreFront

Importante:

- Cuando se usa StoreFront, la aplicación Citrix Workspace para iOS es compatible con las versiones de Citrix Access Gateway Enterprise Edition a partir de la 9.3, y las versiones de Citrix Gateway hasta la 13.
- La aplicación Citrix Workspace para iOS solo ofrece soporte para sitios de XenApp y XenDesktop en la Interfaz Web.
- La aplicación Citrix Workspace para iOS admite el lanzamiento de sesiones desde Workspace para Web, siempre que el explorador web que se utilice funcione con Workspace para Web. Si no puede iniciar sesiones, configure su cuenta a través de la apli-

> cación Citrix Workspace para iOS directamente. Los usuarios deben abrir manualmente el archivo ICA con la función Abrir en Workspace del explorador web. Para conocer las limitaciones de esta implementación, consulte la documentación de StoreFront.

Con StoreFront, los almacenes que se crean consisten en servicios que proporcionan una infraestructura de recursos y autenticación para la aplicación Citrix Workspace para iOS. Cree almacenes que enumeren y agrupen escritorios y aplicaciones de sitios de Citrix Virtual Apps and Desktops y comunidades de Citrix Virtual Apps, lo que habilitará estos recursos para los usuarios.

1. Instale y configure StoreFront. Para obtener información detallada, consulte la documentación de producto de StoreFront. Para los administradores que necesitan más control, Citrix ofrece una plantilla que se puede usar para crear un sitio de descargas para la aplicación Citrix Workspace para iOS.
2. Configure los almacenes para StoreFront tal como lo haría para otras aplicaciones de Citrix Virtual Apps and Desktops. No se requiere ninguna configuración especial para los dispositivos móviles. Para obtener detalles, consulte Opciones de acceso de usuarios en la sección de StoreFront de la documentación de productos. Para dispositivos móviles, use alguno de estos métodos:
    - Archivos de aprovisionamiento. Puede dar a los usuarios unos archivos de aprovisionamiento (.cr) que contienen los datos de conexión con sus almacenes. Después de la instalación, los usuarios abren el archivo en el dispositivo para configurar la aplicación Citrix Workspace para iOS automáticamente. De forma predeterminada, Workspace para sitios web ofrece a los usuarios un archivo de aprovisionamiento para el único almacén para el que esté configurado el sitio en cuestión. También es posible utilizar la consola de administración de Citrix StoreFront con el fin de generar archivos de aprovisionamiento para uno o varios almacenes que se puedan distribuir manualmente a los usuarios.
    - Configuración manual. Es posible informar directamente a los usuarios sobre las direcciones URL de los almacenes o de Citrix Gateway que se necesitan para acceder a sus escritorios y aplicaciones. Para las conexiones a través de Citrix Gateway, los usuarios también deben conocer el método de autenticación requerido y la edición de los productos. Después de la instalación, los usuarios deben introducir estos detalles en la aplicación Citrix Workspace para iOS, que intenta verificar la conexión y, si la conexión es satisfactoria, solicita a los usuarios que inicien sesión.
    - Configuración automática. Toque **Agregar cuenta** en la pantalla de bienvenida e introduzca la URL del servidor StoreFront en el campo de dirección. La configuración de la cuenta tiene lugar inmediatamente cuando se agrega la misma.

Para configurar Citrix Gateway

Si tiene usuarios que se conectan desde fuera de la red interna (por ejemplo, usuarios que se conectan desde Internet o desde ubicaciones remotas), configure la autenticación a través de Citrix Gateway.

- Cuando se usa StoreFront, la aplicación Citrix Workspace para iOS es compatible con las versiones de Citrix Access Gateway Enterprise Edition a partir de la 9.3, y las versiones de Citrix Gateway hasta la 13.

Interfaz Web

Para configurar el sitio de la Interfaz Web, los usuarios con dispositivos iPhone e iPad pueden iniciar aplicaciones a través de dicho sitio y el explorador Safari integrado en sus dispositivos móviles. Configure el sitio de la Interfaz Web de la misma forma que configura otras aplicaciones de Citrix Virtual Apps and Desktops. Si no se ha configurado ningún sitio de XenApp y XenDesktop para el dispositivo móvil, la aplicación Citrix Workspace para iOS usa automáticamente el sitio de la Interfaz Web. No se requiere ninguna configuración especial para los dispositivos móviles.

El explorador Safari integrado admite la Interfaz Web 5.x.

Para iniciar aplicaciones en los dispositivos iOS

En el dispositivo móvil, los usuarios pueden iniciar una sesión en el sitio de la Interfaz Web con sus credenciales normales.

Aprovisionamiento automático para dispositivos móviles

En StoreFront, utilice las tareas “Exportar archivo de aprovisionamiento multialmacén” y “Exportar archivo de aprovisionamiento” para generar archivos que contengan datos de conexión para los almacenes, incluidas las implementaciones de Citrix Gateway y las balizas configuradas para dichos almacenes. Ponga estos archivos a disposición de los usuarios para permitirles que configuren la aplicación Citrix Workspace para iOS automáticamente con la información de los almacenes. Los usuarios también pueden obtener los archivos de aprovisionamiento de la aplicación Citrix Workspace para iOS desde los sitios de Workspace para Web.

> **Importante:**
>
> En implementaciones con varios servidores, use solo un servidor a la vez para hacer cambios en la configuración del grupo de servidores. Compruebe que la consola de administración de Citrix StoreFront no se está ejecutando en ninguno de los demás servidores de la implementación. Una vez completados, propague los cambios de configuración al grupo de servidores de modo que los demás servidores de la implementación se actualicen.

1. En la pantalla Inicio o Aplicaciones de Windows, busque el icono de Citrix StoreFront y haga clic en él. Seleccione el nodo Almacenes en el panel izquierdo de la consola de administración de Citrix StoreFront.

2. Para generar un archivo de aprovisionamiento que contenga información de varios almacenes, en el panel Acciones, haga clic en Exportar archivo de aprovisionamiento multialmacén y seleccione los almacenes que quiera incluir en el archivo.
3. Haga clic en Exportar y en Guardar para guardar el archivo de aprovisionamiento con la extensión `.cr` en una ubicación adecuada de la red.

Información de acceso de usuario

Debe facilitar a los usuarios la información de cuenta de la aplicación Citrix Workspace para iOS que necesitan para poder acceder a sus aplicaciones, escritorios y datos alojados en servidores. Puede proporcionarles esta información de las siguientes formas:

- Configurar la detección de cuentas basada en direcciones de correo electrónico
- Proporcionar un archivo de aprovisionamiento a los usuarios
- Proporcionar información de cuenta a los usuarios para que la introduzcan manualmente

Configurar la detección de cuentas basada en direcciones de correo electrónico

Puede configurar la aplicación Citrix Workspace para iOS para que use la detección de cuentas basada en correo electrónico. Cuando está configurada, los usuarios introducen su dirección de correo electrónico, en lugar de una dirección URL de servidor, durante la instalación y configuración inicial de la aplicación Citrix Workspace para iOS. La aplicación Citrix Workspace para iOS determina el servidor Access Gateway o StoreFront, o bien el dispositivo virtual de Endpoint Management, que está asociado a esa dirección de correo electrónico en función de los registros del servicio (SRV) que contiene el sistema de nombres de dominio (DNS). A continuación, pide a los usuarios que inicien la sesión para acceder a sus aplicaciones, escritorios y datos alojados en servidores.

> **Nota:**
>
> La detección de cuentas por correo electrónico no se ofrece si la aplicación Citrix Workspace para iOS se conecta a una implementación de Interfaz Web.

Entrega de un archivo de aprovisionamiento a los usuarios

Es posible utilizar StoreFront para crear archivos de aprovisionamiento que contengan los detalles de conexión de las cuentas. Usted pone estos archivos a disposición de los usuarios para que puedan configurar la aplicación Citrix Workspace para iOS de forma automática. Después de instalar la aplicación Citrix Workspace para iOS, los usuarios solo tienen que abrir el archivo `.cr` en el dispositivo para configurar la aplicación Citrix Workspace para iOS. Si se configuran sitios de Workspace para Web, los usuarios también pueden obtener los archivos de aprovisionamiento de la aplicación Citrix Workspace para iOS desde esos sitios.

Para obtener más información, consulte la documentación de StoreFront.

Proporcionar información de cuenta a los usuarios para que la introduzcan manualmente

Si va a entregar a los usuarios los datos de sus cuentas para que luego los introduzcan manualmente, asegúrese de distribuir la siguiente información para permitirles conectar con éxito con sus aplicaciones y escritorios alojados en servidores:

- La dirección URL de StoreFront o del sitio de XenApp y XenDesktop que aloja los recursos; por ejemplo, `servername.company.com`.
- Para accesos mediante Citrix Gateway, proporcione la dirección de Citrix Gateway y el método de autenticación requerido.

Cuando un usuario introduce la información de una cuenta nueva, la aplicación Citrix Workspace para iOS intenta verificar la conexión. Si la conexión puede establecerse, la aplicación Citrix Workspace para iOS solicita al usuario que inicie sesión en la cuenta.

Configuración

September 15, 2020

Guardar contraseñas

Mediante la consola de administración de la Interfaz Web de Citrix, puede configurar el método de autenticación para permitir que los usuarios guarden sus contraseñas. Cuando se configura la cuenta de usuario, la contraseña cifrada se guarda hasta que el usuario se conecta por primera vez. Se deben tener en cuenta las siguientes cuestiones:

- Si se habilita el almacenamiento de contraseñas, la aplicación Citrix Workspace para iOS almacena la contraseña en el dispositivo para inicios de sesión futuros y ya no se solicitan las contraseñas cuando los usuarios se conectan con las aplicaciones.

  > **Nota:**
  >
  > La contraseña se almacena solamente si los usuarios introducen una contraseña cuando se crea una cuenta. Si no se introduce una contraseña para la cuenta, no se guarda ninguna contraseña, independientemente de cómo se haya configurado este parámetro en el servidor.

- Si se inhabilita el almacenamiento de contraseñas (configuración predeterminada), la aplicación Citrix Workspace para iOS solicita a los usuarios que introduzcan sus contraseñas cada vez que se conectan.

> **Nota:**
>
> Para conexiones directas con StoreFront, no es posible guardar la contraseña.

Para anular el parámetro de almacenamiento de contraseñas

Si se configura el servidor para que almacene las contraseñas, los usuarios que prefieran que les sean solicitadas las mismas cada vez que inician una sesión pueden anular dicho parámetro:

- Al crear la cuenta, deje el campo de contraseña en blanco.
- Al modificar la cuenta, elimine la contraseña y guarde la cuenta.

Usar la función Guardar contraseña

La aplicación Citrix Workspace para iOS tiene una función que simplifica el proceso de conexión, ya que permite guardar la contraseña, lo que elimina el paso adicional de tener que autenticar una sesión cada vez que se abre la aplicación.

> **Nota:**
>
> Actualmente la funcionalidad para guardar contraseñas admite el protocolo PNA. No admite el modo *nativo* de StoreFront. Sin embargo, esta funcionalidad está operativa cuando StoreFront habilita el modo *antiguo* de PNA.

Configurar StoreFront

Para configurar StoreFront para poder habilitar la función Guardar contraseña:

1. Si configura un almacén existente, vaya al paso 3.
2. Para configurar una nueva implementación de StoreFront, siga las prácticas recomendadas descritas en Instalar, configurar y desinstalar Citrix StoreFront.
3. Abra la consola de administración de Citrix StoreFront. Asegúrese de que la URL base usa HTTPS y es la misma que el nombre común especificado al generar el certificado SSL.
4. Seleccione el almacén que quiere configurar.
5. Haga clic en **Configurar soporte de servicios XenApp**.
6. Habilite la **compatibilidad con el servicio XenApp**, seleccione el **almacén predeterminado**(opcional) y haga clic en **Aceptar**.
7. Vaya al archivo de plantilla de configuración ubicado en c:\inetpub\wwwroot\Citrix\<nombre del almacén>\Views\PnaConfig\.
8. Haga una copia de seguridad del archivo Config.aspx.

9. Abra el archivo Config.aspx.
10. Modifique la línea <EnableSavePassword>**false**</EnableSavePassword>: cambie el valor **false** a **true**.
11. Guarde el archivo Config.aspx modificado.
12. En el servidor de StoreFront, ejecute PowerShell con derechos de administrador.
13. En la consola PowerShell:

    a. cd “c:\Archivos de programa\Citrix\Receiver StoreFront\Scripts”

    b. Escriba “Set-ExecutionPolicy RemoteSigned”

    c. Escriba “.\ImportModules.ps1”

    d. Escriba “Set-DSServiceMonitorFeature –ServiceUrl” `https://localhost:443/StorefrontMonitor`
14. Si tiene un grupo de StoreFront, ejecute los mismos comandos en todos los miembros del grupo.

Configurar Citrix Gateway para guardar contraseñas

> **Nota:**
>
> Esta configuración usa servidores de equilibrio de carga de Citrix Gateway.

Para configurar Citrix Gateway con el objetivo de ofrecer la función Guardar contraseña:

1. Inicie sesión en la consola de administración de Citrix Gateway.
2. Siga la práctica recomendada por Citrix para crear un certificado para los servidores virtuales de equilibrio de carga.
3. En la ficha de configuración, vaya a Traffic Management -> Load Balancing -> Servers y haga clic en **Add**.
4. Introduzca el nombre y la dirección IP del servidor de StoreFront.
5. Haga clic en **Create**. Si tiene un grupo de StoreFront, repita el paso 5 en cada uno de los servidores del grupo.
6. En la ficha de configuración, vaya a **Traffic Management** -> **Load Balancing** -> **Monitor** y haga clic en **Add**.
7. Introduzca un nombre para el monitor. Seleccione **STOREFRONT** como tipo (Type). En la parte inferior de la página, seleccione **Secure** (es necesario porque el servidor de StoreFront usa HTTPS).
8. Haga clic en la ficha **Special Parameters**. Introduzca el nombre de StoreFront configurado anteriormente, seleccione **Check Backed Services** y haga clic en **Create**.

9. En la ficha **Configuration**, vaya a **Traffic Management** > **Load Balancing** > **Service Groups** y haga clic en **Add**.
10. Introduzca un nombre para el grupo de servicios, establezca el protocolo en **SSL** y haga clic en **OK**.
11. En la parte derecha de la pantalla, en la sección Advanced Settings, seleccione **Settings**.
12. Habilite la IP de cliente, introduzca lo siguiente como valor de encabezado: **X-Forwarded-For** y haga clic en **OK**.
13. En la parte derecha de la pantalla, en la sección Advanced Settings, seleccione **Monitors**. Haga clic en la flecha para agregar nuevos monitores.
14. Haga clic en el botón **Add** y, a continuación, seleccione el menú desplegable **Select Monitor**. Aparecerá una lista de monitores (los configurados en Citrix Gateway).
15. Haga clic en el botón de opción situado junto a los monitores que creó anteriormente y haga clic en **Select** y, a continuación, en **Bind**.
16. En la parte derecha de la pantalla (en la sección Advanced Settings), seleccione **Members**. Haga clic en la flecha para agregar nuevos miembros del grupo de servicios.
17. Haga clic en el botón **Add** y, a continuación, seleccione la lista desplegable **Select Member**.
18. Seleccione el botón de opción **Server Based**. Aparecerá una lista de miembros del servidor (los configurados en Citrix Gateway). Haga clic en el botón de opción junto a los servidores de StoreFront que creó anteriormente.
19. Introduzca 443 como número de puerto y especifique un número exclusivo para el ID de hash. A continuación, haga clic en **Create** y en **Done**. Si todo se ha configurado correctamente, en **Effective State** aparecerá una luz verde, lo que indica que la supervisión está funcionando adecuadamente.
20. Vaya a Traffic Management -> Load Balancing -> Virtual Servers y haga clic en **Add**. Introduzca un nombre para el servidor y seleccione **SSL** como protocolo.
21. Introduzca la dirección IP del servidor de StoreFront de carga equilibrada y haga clic en **OK**.
22. Seleccione el vínculo **Load Balancing Virtual Server Service Group**, haga clic en la flecha y agregue el grupo de servicios creado previamente. Haga clic en **OK** dos veces.
23. Asigne el certificado SSL creado para el servidor virtual de equilibrio de carga. Seleccione **No Server Certificate**.
24. Seleccione el certificado del servidor de equilibrio de carga en la lista y haga clic en **Bind**.
25. Agregue el certificado de dominio al servidor de equilibrio de carga. Haga clic en **No CA certificate**.
26. Seleccione el certificado de dominio y haga clic en **Bind**.

27. En el lado derecho de la pantalla, seleccione **Persistence**.
28. Cambie el valor de Persistence a **SOURCEIP** y establezca el tiempo de espera en **20**. Haga clic en **Save** y luego en **Done**.
29. En el servidor DNS del dominio, agregue el servidor de equilibrio de carga (si aún no se ha creado).
30. Inicie la aplicación Citrix Workspace para iOS en el dispositivo iOS e introduzca la URL completa de XenApp.

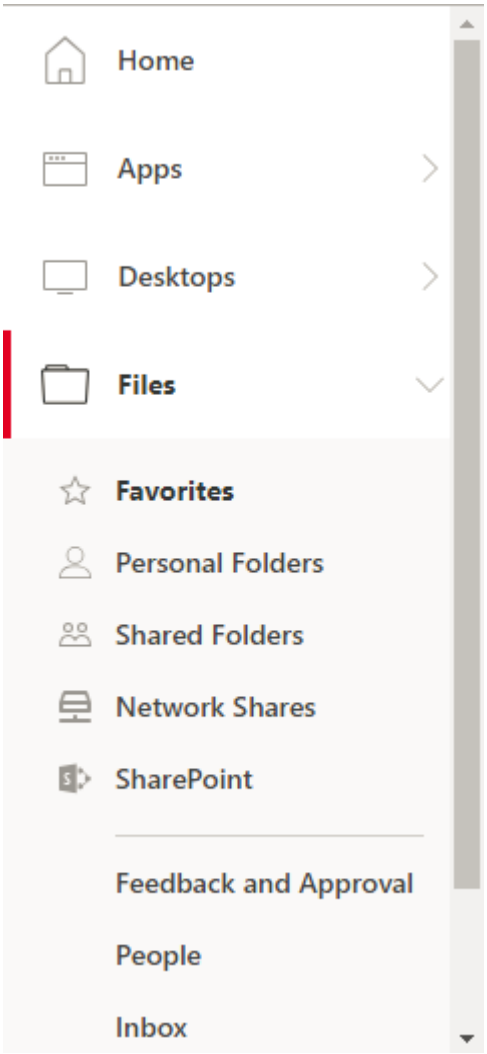
Integración de Content Collaboration Service

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 se muestra 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 se admite en Windows Server 2012 y Windows Server 2016 debido a una opción de seguridad establecida en el sistema operativo.

La imagen siguiente muestra el contenido de ejemplo de la ficha Archivos en 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.

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 iOS y envía esos datos automáticamente a Google Firebase.	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 según se especifique en el anexo de seguridad de Citrix Services, disponible en el Centro de confianza de Citrix.

Citrix utiliza Google Firebase para recopilar determinados datos de la aplicación Citrix Workspace como parte del programa CEIP. Consulte cómo Google gestiona los datos recopilados para Google Firebase.

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

1. Abra la aplicación Citrix Workspace para iOS.
2. Toque **Inicio** > **Parámetros**.
3. Vaya a la sección **General**.
4. Inhabilite la opción **Enviar estadísticas de uso**.

Los elementos específicos de los datos de CEIP que recopila Google Firebase son:

Información de sesión y método de inicio de sesión	Almacenes de Citrix y configuración de los almacenes	Tipo de autenticación y configuración de la autenticación	Conexiones ICA
Inicio de sesiones HDX	Sesión de aplicación de almacén	Acción abierta de WebView	Copia de acciones de WebView

Uso compartido de acciones de WebView	Revisión de la aplicación Workspace	Estado de las conexiones, errores de conexión, uso del centro de conexiones	Pantalla externa
Estado de los sockets	Duración de las sesiones	HDX a través de UDP	Hora de los inicios de sesión
Información de dispositivos	Información del modelo del dispositivo	Enviar estadísticas de uso	Idioma de la aplicación y de la aplicación Workspace
Idioma del teclado	Tipo de almacén de Citrix	Combinación de almacenes de Citrix	Tipo de protocolo de los almacenes
Recuento de almacenes	Estado de HDX a través de UDP	Instalaciones de tokens RSA	

Citrix Ready Workspace Hub

Citrix Ready Workspace Hub combina entornos digitales y físicos para entregar aplicaciones y datos dentro de un espacio inteligente y seguro. El sistema completo conecta dispositivos (o cosas), como aplicaciones móviles y sensores, para crear un entorno inteligente que responda adecuadamente.

Citrix Ready Workspace Hub se ha construido sobre la plataforma Raspberry Pi 3. El dispositivo que ejecuta la aplicación Citrix Workspace se conecta a Citrix Ready Workspace Hub y transmite las aplicaciones o los escritorios hacia una pantalla más grande.

Para obtener más información sobre Citrix Ready Workspace Hub, consulte la documentación de Citrix Ready Workspace Hub.

Por motivos de seguridad, Citrix Ready Workspace Hub admite conexiones SSL con dispositivos móviles. Establezca un nombre de dominio completo (FQDN) de manera manual o automática para identificar de forma única cada dispositivo. Para obtener más información, consulte Conexión de seguridad en la documentación de Citrix Ready Workspace Hub.

Citrix Ready Workspace Hub se habilita en la aplicación Citrix Workspace cuando se cumplen todos los requisitos de sistema siguientes:

- Aplicación Citrix Workspace 1810.1 para iOS o versiones posteriores
- Bluetooth habilitado
- El dispositivo móvil y Workspace Hub deben utilizar la misma red Wi-Fi

Configuración

Para activar las funciones del concentrador de Citrix Ready Workspace Hub, vaya a **Parámetros** y toque **Citrix Casting** para habilitar la función en su dispositivo. Para obtener más información, consulte la documentación de ayuda para dispositivos iOS.

La aplicación Citrix Workspace integra un nuevo procedimiento para agregar o quitar un Workspace Hub de la lista de confianza en dispositivos iOS. Para obtener más información, consulte Conexión de seguridad.

Limitación conocida

- En VDA 7.18 y versiones anteriores, la conversión a un Workspace Hub requiere que el escritorio u otro recurso que esté utilizando tenga habilitada la directiva de pantalla completa .h264 y que la directiva de gráficos antiguos esté inhabilitada.

Sesiones compartidas

Cuando los usuarios cierran la sesión de una cuenta de la aplicación Citrix Workspace para iOS, si aún tienen conexiones con aplicaciones o escritorios, pueden elegir entre desconectarse o cerrar la sesión:

- **Desconectar**: Cierra la sesión de la cuenta, pero deja la aplicación o el escritorio de Windows activos en el servidor. El usuario puede iniciar después otro dispositivo, abrir la aplicación Citrix Workspace para iOS y volver a conectarse con el último estado que tenía antes de desconectarse del dispositivo iOS. Esta opción permite a los usuarios reconectarse desde un dispositivo a otro y reanudar el trabajo con las aplicaciones en ejecución.
- **Cerrar sesión**: Cierra la sesión de la cuenta, cierra la aplicación Windows y cierra la sesión en el servidor Citrix Virtual Apps and Desktops. Esta opción permite a los usuarios desconectarse del servidor y cerrar la sesión de la cuenta. Cuando vuelven a iniciar la aplicación Citrix Workspace para iOS, esta se abre en el estado predeterminado.

Workspace con funciones inteligentes

A partir de la versión 1911, la aplicación está optimizada para aprovechar las próximas funciones inteligentes cuando estas se publiquen. Para obtener más información, consulte Funciones inteligentes de Workspace: Microaplicaciones.

Compatibilidad con iOS 13 y iPadOS

La aplicación Citrix Workspace para iOS es compatible con iOS 13 y iPadOS, incluida la función multitarea de iPadOS.

> **Importante:**
>
> - La aplicación CR01 no está disponible en iOS 13. Si está utilizando la aplicación CR01, Citrix recomienda no actualizar a iOS 13.
> - Si utiliza la cadena de certificados SHA-1, es posible que tenga que pasarse a la cadena de certificados SHA-2. Los certificados firmados SHA-1 ya no son de confianza en iOS 13. Para obtener más información sobre los certificados de servidor TLS, consulte Requisitos para certificados de confianza en iOS 13 y macOS 10.15.
> - En iOS 13, el inicio de sesiones desde el explorador web Safari ha cambiado. Para obtener más información, consulte la documentación de ayuda.

Con la función AssistiveTouch, ahora la aplicación Citrix Workspace para iOS se conecta al dispositivo Citrix X1 Mouse de otra manera. La aplicación Citrix Workspace ya no se conecta al Citrix X1 Mouse en el inicio. Por lo tanto, el icono de Citrix X1 Mouse ya no está disponible en la barra de herramientas junto al icono Configuración. Para ver si se ha habilitado el acceso a un dispositivo Citrix X1 Mouse emparejado para la aplicación Citrix Workspace, vaya a **Configuración** > **Citrix X1 Mouse**.

Itinerancia de sesión en iPad

A partir de la versión 1906, la itinerancia de sesiones está disponible en dispositivos táctiles iPhone y iPad al utilizar un almacén en la nube. Para obtener más información, consulte la documentación de ayuda de Dispositivos iOS.

Sincronización de la distribución de teclado

La sincronización de la distribución del teclado permite a los usuarios cambiar distribuciones de teclado preferidas en el dispositivo cliente. Esta función está inhabilitada de forma predeterminada.

Para habilitar la sincronización de la distribución de teclado, vaya a **Parámetros** > **Opciones de teclado** y habilite la opción **Sincronización de distribución de teclado**.

> **Nota:**
>
> El uso de la opción de distribución de teclado local activa el IME (Input Method Editor) del cliente. Si usted trabaja en japonés, chino o coreano y prefiere usar el editor IME del servidor, inhabilite la opción de distribución de teclado local en **Preferencias** > **Teclado**.

Redirección del host al cliente

La redirección de contenido permite controlar si los usuarios acceden a la información desde aplicaciones publicadas en servidores o desde aplicaciones que se ejecutan localmente en dispositivos de usuario.

La redirección del host al cliente es un tipo de redirección de contenido. Solo se admite en agentes VDA de SO de servidor (no en agentes VDA de SO de escritorio).

Cuando la redirección del host al cliente está habilitada, las direcciones URL se interceptan en el servidor VDA y se envían al dispositivo de usuario. El explorador web o el reproductor multimedia presentes en el dispositivo de usuario abren esas direcciones URL. Si habilita la redirección de host a cliente y el dispositivo del usuario no puede conectarse a una URL, dicha URL se redirige de nuevo al VDA del servidor. Cuando la redirección del host al cliente está inhabilitada, los usuarios pueden abrir las URL con exploradores web o reproductores multimedia que residan en el VDA de servidor.
Cuando la redirección de host a cliente está habilitada, los usuarios no pueden inhabilitarla.

Anteriormente, la redirección del host al cliente recibía el nombre de redirección del servidor al cliente.

Para obtener más información, consulte Redirección de contenido general.

Funcionalidad de credenciales derivadas de Purebred

A partir de la versión 1810, la aplicación Citrix Workspace para iOS admite credenciales derivadas de Purebred. Al conectarse a un almacén que permite credenciales derivadas, los usuarios pueden iniciar sesión en la aplicación Citrix Workspace para iOS con una tarjeta inteligente virtual. Esta función solo está disponible en implementaciones locales.

> **Nota:**
>
> Se requiere Citrix Virtual Apps and Desktops 7 1808 o versiones posteriores para usar esta función.

Para obtener información sobre la configuración de credenciales derivadas, consulte Credenciales derivadas.

Autenticarse

August 17, 2020

Autenticación de certificados de cliente

> **Importante:**
>
> - Cuando se utiliza StoreFront, la aplicación Citrix Workspace para iOS admite:
>   - Citrix Access Gateway Enterprise Edition 9.3
>   - NetScaler Gateway de la versión 10.x a la versión 11.0
>   - Citrix Gateway 11.1 y versiones posteriores.

- La autenticación con certificados del cliente se admite en la aplicación Citrix Workspace para iOS.
- Solo Access Gateway Enterprise Edition 9.x y 10.x (y versiones posteriores) admiten la autenticación con certificados del cliente.
- Los tipos de autenticación de doble origen deben ser CERT y LDAP.
- La aplicación Citrix Workspace para iOS también admite la autenticación opcional con certificados del cliente.
- Solo se admiten certificados con formato P12.

Los usuarios que inician sesiones en un servidor Citrix Gateway virtual pueden ser autenticados también basándose en los atributos del certificado del cliente que se presenta ante el servidor virtual. La autenticación con certificados del cliente también puede utilizarse con otro tipo de autenticación, LDAP, para ofrecer autenticación de doble origen.

Para autenticar usuarios basándose en los atributos del certificado del cliente, la autenticación de clientes debe estar habilitada en el servidor virtual y se debe solicitar el certificado del cliente. Es necesario vincular un certificado raíz al servidor virtual en Citrix Gateway.

Cuando los usuarios inician sesiones en el servidor Citrix Gateway virtual, después de la autenticación, la información de nombre de usuario y dominio se extrae del campo especificado del certificado. Esta información debe estar en el campo **SubjectAltName:OtherName:MicrosoftUniversalPrincipalName** del certificado. Está en el formato "nombreDeUsuario@dominio". Si el nombre de usuario y el dominio se extraen correctamente, y el usuario suministra la otra información requerida (por ejemplo, una contraseña), se autenticará al usuario. Si el usuario no presenta un certificado y credenciales válidas, o si falla la extracción del nombre de usuario y el dominio, la autenticación también fallará.

Se puede autenticar usuarios basándose en el certificado del cliente, definiendo el tipo de autenticación predeterminado para que use el certificado del cliente. También se puede crear una acción de certificado que defina lo que hay que hacer durante la autenticación basada en un certificado SSL del cliente.

Para configurar el sitio de servicios XenApp

Si aún no ha creado un sitio de servicios XenApp, en la consola de Citrix Virtual Apps o en la consola de la Interfaz Web (según la versión de Citrix Virtual Apps instalada), cree un sitio de servicios XenApp para dispositivos móviles.

El software de la aplicación Citrix Workspace para iOS para dispositivos móviles utiliza un sitio de servicios XenApp para obtener información sobre las aplicaciones a las que un usuario tiene derecho, y las presenta en la aplicación que se ejecuta en el dispositivo. Esto es similar al modo en que se utiliza la Interfaz Web para las conexiones tradicionales de Citrix Virtual Apps basadas en SSL para las que se puede configurar un dispositivo Citrix Gateway.

Configure el sitio de servicios XenApp para que la aplicación Citrix Workspace para iOS para dispositivos móviles admita conexiones provenientes de una conexión de Citrix Gateway.

1. En el sitio de servicios XenApp, seleccione **Manage secure client access > Edit secure client access** settings.
2. Cambie el método de acceso a Direct con Gateway.
3. Escriba el nombre de dominio completo del dispositivo Citrix Gateway.
4. Escriba la información de Secure Ticket Authority (STA).

Para configurar el dispositivo Citrix Gateway

La autenticación con el certificado del cliente requiere configurar Citrix Gateway con la autenticación de dos factores mediante dos directivas de autenticación: Cert y LDAP.

1. Cree una directiva de sesión en Citrix Gateway para permitir las conexiones entrantes de Citrix Virtual Apps desde la aplicación Citrix Workspace para iOS y especifique la ubicación del sitio de servicios XenApp creado recientemente.

    - Cree una directiva de sesión nueva para identificar que la conexión proviene de la aplicación Citrix Workspace para iOS para dispositivos móviles. Cuando cree la directiva de sesión, configure la siguiente expresión y elija Hacer coincidir todas las expresiones como el operador de la expresión:

      REQ.HTTP.HEADER User-Agent CONTAINS CitrixWorkspace

    - En la configuración del perfil asociado para la directiva de sesión, en la ficha Security, configure Default Authorization con el valor Allow (Permitir).

      En la ficha “Published Applications”, si no es un parámetro global (es decir, la casilla “Override Global” está marcada), compruebe que el campo “ICA Proxy” esté desactivado.

      En el campo “Web Interface Address”, escriba la dirección URL, incluido el archivo config.xml, del sitio de servicios XenApp que utilizan los usuarios del dispositivo; por ejemplo, //XenAppServerName/Citrix/PNAgent/config.xml o /XenAppServerName/CustomPath/config.xml.

    - Vincule la directiva de sesión con un servidor virtual.
    - Cree directivas de autenticación para Cert y LDAP.
    - Vincule las directivas de autenticación con el servidor virtual.
    - Configure el servidor virtual para que solicite certificados de cliente en la conexión TLS (en la ficha Certificate (Certificado), abra SSL Parameters (Parámetros SSL), y para Client Authentication (Autenticación de cliente), defina Client Certificate (Certificado del cliente) como Mandatory (Obligatorio).

> **Importante:**
>
> Si el certificado de servidor que se utiliza en Citrix Gateway forma parte de una cadena de certificados (con un certificado intermedio), compruebe que los certificados intermedios también estén instalados correctamente en Citrix Gateway. Para obtener más información sobre la instalación de certificados, consulte la documentación de Citrix Gateway.

Para configurar el dispositivo móvil

Si la autenticación de certificados del cliente está habilitada en Citrix Gateway, los usuarios se autenticarán basándose en ciertos atributos del certificado del cliente. Una vez completada con éxito la autenticación, el nombre de usuario y el dominio se extraen del certificado y se aplican las directivas especificadas para dicho usuario.

1. En la aplicación Citrix Workspace para iOS, abra la cuenta y, en el campo "Servidor", introduzca el nombre FQDN correspondiente a su servidor Citrix Gateway, por ejemplo, ServidorCertificadosClienteGateway.empresa.com. La aplicación Citrix Workspace para iOS detecta automáticamente que se necesita el certificado del cliente.
2. Los usuarios pueden instalar un certificado nuevo o bien seleccionar uno de la lista de certificados ya instalados. La autenticación con certificado del cliente iOS requiere que solo la aplicación Citrix Workspace para iOS descargue e instale el certificado.
3. Después de seleccionar un certificado válido, los campos de nombre de usuario y dominio en la pantalla de inicio de sesión se rellenan con la información del nombre de usuario del certificado, y los usuarios introducen la información restante, incluida la contraseña.
4. Si la autenticación con certificado del cliente es optativa, los usuarios pueden omitir la selección de certificado. Para ello, deberán presionar el botón Atrás en la página de certificados. En este caso, la aplicación Citrix Workspace para iOS continúa con la conexión y presenta al usuario la pantalla de inicio de sesión.
5. Después de que los usuarios completan el inicio de sesión, pueden iniciar las aplicaciones sin tener que proporcionar el certificado nuevamente. La aplicación Citrix Workspace para iOS almacena el certificado de la cuenta y lo utiliza automáticamente para solicitudes de inicio de sesión futuras.

Tarjetas inteligentes

La aplicación Citrix Workspace para iOS admite el uso de tarjetas inteligentes SITHS solo en conexiones dentro de la sesión.

Si usa dispositivos Citrix Gateway FIPS, configure sus sistemas para rechazar renegociaciones SSL. Para obtener información detallada, consulte el artículo CTX123680 de Citrix Knowledge Center.

Se admiten los productos y las configuraciones siguientes:

- Lectores admitidos:
  - Precise Biometrics Tactivo para iPad Mini Firmware versión 3.8.0
  - Precise Biometrics Tactivo para iPad (4.ª generación) y Tactivo para iPad (3.ª generación) y iPad 2 Firmware versión 3.8.0
  - Lectores de tarjeta inteligente BaiMobile® 301MP y 301MP-L
- Respaldo de middleware de tarjeta inteligente para VDA
  - ActiveIdentity
- Tarjetas inteligentes admitidas:
  - Tarjetas PIV
  - Tarjetas CAC (Common Access Card)
- Configuraciones admitidas:
  - Autenticación con tarjeta inteligente en Citrix Gateway con StoreFront 2.x y XenDesktop 7.x o versiones posteriores, o XenApp 6.5 o versiones posteriores

Cómo configurar la aplicación Citrix Workspace para iOS para acceder a aplicaciones

1. Si quiere configurar la aplicación Citrix Workspace para iOS para acceder automáticamente a aplicaciones al crear una cuenta, introduzca la URL de su almacén en el campo “Dirección”; por ejemplo, storefront.empresa.com o netscalervserver.empresa.com.
2. Seleccione la opción **Usar tarjeta inteligente** cuando vaya a utilizar una tarjeta inteligente para la autenticación.

> **Nota:**
>
> Los inicios de sesión en un almacén son válidos durante una hora aproximadamente. Transcurrido ese tiempo, los usuarios tienen que volver a iniciar una sesión para actualizar o iniciar sus aplicaciones.

Autenticación con RSA SecurID

La autenticación con RSA SecurID para la aplicación Citrix Workspace para iOS es compatible con las configuraciones de Secure Web Gateway (mediante la Interfaz Web solamente) y todas las configuraciones de Citrix Gateway.

Se requiere un esquema de URL para el token de software en la aplicación Citrix Workspace para iOS: El token de software de RSA SecurID usado por la aplicación Citrix Workspace para iOS registra solamente el esquema de URL com.citrix.securid.

Si los usuarios han instalado las aplicaciones Citrix Workspace para iOS y RSA SecurID en sus dispositivos iOS, deberán seleccionar el esquema de URL “com.citrix.securid” para importar el token de software de RSA SecurID a los dispositivos con la aplicación Citrix Workspace para iOS.

Para importar un token de software de RSA SecurID

Para usar un token de software de RSA con la aplicación Citrix Workspace para iOS, indique a sus usuarios que sigan este procedimiento.

La directiva de longitud de PIN, el tipo de PIN (solo numérico, alfanumérico) y los límites de reutilización de un PIN se especifican en el servidor de administración de RSA.

Los usuarios solo tienen que hacer esto una vez, después de haberse autenticado correctamente en el servidor RSA. Después de que los usuarios verifican su PIN, también se les autentica en el servidor StoreFront y éste les presenta las aplicaciones publicadas y los escritorios disponibles.

Para utilizar un token de software de RSA

1. Importe el token de software de RSA suministrado por su organización.
2. En el mensaje que lleva adjunto el archivo de SecurID, seleccione **Abrir en Workspace** como destino de la importación. Después de importar el token de software, la aplicación Citrix Workspace para iOS se abre automáticamente.
3. Si su organización le proporcionó una contraseña para completar la importación, introdúzcala y haga clic en **Aceptar**. Después de hacer clic en **Aceptar**, verá un mensaje donde se indica que el token se ha importado.
4. Cierre ese mensaje de importación y, en aplicación Citrix Workspace para iOS, haga clic en **Agregar cuenta**.
5. Introduzca la dirección URL del almacén que le haya facilitado su organización y haga clic en **Siguiente**.
6. En la pantalla de inicio de sesión, escriba sus credenciales (nombre de usuario, contraseña y dominio). En el campo PIN, introduzca **0000**, a menos que su organización le haya facilitado otro PIN predeterminado. (El PIN 0000 es el predeterminado de RSA, pero es posible que su organización lo cambie por otro, para cumplir con sus directivas de seguridad).
7. En la parte superior izquierda, haga clic en **Iniciar sesión**. Después de hacer clic en el botón **Iniciar sesión**, se le pedirá que cree un PIN nuevo.
8. Introduzca un PIN de entre 4 y 8 dígitos, y haga clic en **Aceptar**.
9. A continuación se le pedirá que verifique el nuevo PIN. Vuelva a introducir su PIN y haga clic en **Aceptar**. Después de hacer clic en Aceptar, podrá acceder a sus aplicaciones y escritorios.

Siguiente tokencode

Si configura Citrix Gateway para la autenticación de RSA SecurID, la aplicación Citrix Workspace para iOS admite el modo Siguiente tokencode. Si esta función está habilitada, cuando un usuario introduce

la contraseña incorrecta tres veces (valor predeterminado), Citrix Gateway plug-in solicita al usuario que espere hasta que se active el próximo token antes de iniciar una sesión. Asimismo, el servidor RSA se puede configurar para inhabilitar una cuenta de usuario si el usuario intenta iniciar una sesión demasiadas veces con la contraseña incorrecta.

Credenciales derivadas

Las credenciales derivadas de Purebred dentro de la aplicación Citrix Workspace para iOS están disponibles. Al conectarse a un almacén que permite credenciales derivadas, los usuarios pueden iniciar sesión en la aplicación Citrix Workspace para iOS con una tarjeta inteligente virtual. Esta función solo está disponible en implementaciones locales.

> **Nota:**
>
> Se requiere Citrix Virtual Apps and Desktops 7 1808 o versiones posteriores para usar esta función.

Para habilitar las credenciales derivadas en la aplicación Citrix Workspace para iOS:

1. Vaya a **Parámetros > Avanzado> Credenciales derivadas**.
2. Toque **Credenciales derivadas**.

Luego, para crear una tarjeta inteligente virtual que admita credenciales derivadas:

1. En **Parámetros > Avanzado> Credenciales derivadas**, toque **Agregar nueva tarjeta inteligente virtual**.
2. Modifique el nombre de la tarjeta inteligente virtual.
3. Introduzca un PIN de solo 8 dígitos numéricos y confírmelo.
4. Toque **Siguiente**.
5. En Certificado de autenticación, toque **Importar certificado…**
6. Aparece el selector de documentos. Toque **Examinar**.
7. En Ubicaciones, seleccione **Llavero de Purebred**.
8. Seleccione el certificado de autenticación que desee de la lista.
9. Toque **Importar clave**.
10. Repita los pasos 5 a 9 para el Certificado de firma digital y el Certificado de cifrado, si lo desea.
11. Toque **Guardar**.

Puede importar hasta tres certificados para su tarjeta inteligente virtual. El certificado de autenticación es necesario para que la tarjeta inteligente virtual funcione correctamente. El certificado de cifrado y el certificado de firma digital se pueden agregar para usarlos dentro de una sesión VDA.

> **Nota:**
>
> Al conectarse a una sesión HDX, la tarjeta inteligente virtual creada se redirige a la sesión.

Limitaciones conocidas

- Los usuarios solo pueden tener una tarjeta activa a la vez.
- Una vez que se haya creado una tarjeta inteligente virtual, no se puede modificar. Para realizar cambios en la tarjeta inteligente virtual, los usuarios deben eliminar la tarjeta y crear una nueva.
- Puede introducir un PIN inválido hasta 10 veces. Después del décimo intento, la tarjeta inteligente virtual se elimina.
- Cuando se seleccionan las credenciales derivadas, la tarjeta inteligente virtual creada anteriormente reemplaza una tarjeta inteligente física cuando se necesita una tarjeta inteligente en una sesión.

Protección

August 17, 2020

Para proteger la comunicación entre la comunidad de servidores y la aplicación Citrix Workspace para iOS, puede integrar las conexiones a la comunidad de servidores con la ayuda de diversas tecnologías de seguridad, incluido Citrix Gateway.

> **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 la aplicación Citrix Workspace para iOS y los servidores. La aplicación Citrix Workspace para iOS admite el uso de SOCKS y protocolos de proxy seguro.
- Secure Web Gateway Puede utilizar Secure Web Gateway junto con la Interfaz Web 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 utiliza la aplicación Citrix Workspace para iOS 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.

Citrix Gateway

Para permitir que los usuarios remotos se conecten a su implementación de Citrix Endpoint Management mediante Citrix Gateway, puede configurar los certificados para que funcionen con StoreFront. El método que se debe utilizar para habilitar el acceso depende de la edición de Citrix Endpoint Management existente en la implementación.

Si implementa Citrix Endpoint Management en la red, integre Citrix Gateway con 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 para iOS.

Secure Web Gateway

Este tema solo se aplica a entornos donde se usa la Interfaz Web.

Es posible usar Secure Web Gateway en modo Normal o en modo Relay (Traspaso) para proporcionar un canal de comunicaciones seguro entre la aplicación Citrix Workspace para iOS y el servidor. No es necesario configurar la aplicación Citrix Workspace para iOS si se utiliza Secure Web Gateway en el modo Normal y los usuarios se conectan a través de la Interfaz Web.

La aplicación Citrix Workspace para iOS usa parámetros que se configuran de forma remota en el servidor de la Interfaz Web para conectarse con los servidores que ejecutan Secure Web Gateway.

Si se instala Secure Web Gateway Proxy en un servidor de una red segura, se puede utilizar Secure Web Gateway Proxy en modo de traspaso (Relay). Si se utiliza el modo Relay, el servidor Secure Web Gateway funciona como un proxy y es necesario configurar la aplicación Citrix Workspace para iOS para que use lo siguiente:

- El nombre de dominio completo (FQDN) del servidor Secure Web Gateway.
- El número de puerto del servidor Secure Web Gateway. Tenga en cuenta que el modo Relay no se ofrece en la versión 2.0 de Secure Web Gateway.

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

- Nombre de host
- Dominio intermedio
- Dominio superior

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

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 iOS y los servidores. La aplicación Citrix Workspace para iOS admite tanto el uso de SOCKS como el de protocolos de proxy seguro.

En la comunicación con el servidor Citrix Virtual Apps and Desktops, la aplicación Citrix Workspace para iOS utiliza los parámetros del servidor proxy configurados de forma remota en el servidor de la Interfaz Web.

En la comunicación con el servidor web, la aplicación Citrix Workspace para iOS utiliza los parámetros del servidor proxy configurados para el explorador web predeterminado en el dispositivo de usuario. Se deben configurar los parámetros del servidor proxy para el explorador web predeterminado en el dispositivo de usuario según corresponda.

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 se utiliza un firewall en el entorno, la aplicación Citrix Workspace para iOS debe poder comunicarse a través de este con el servidor web y el servidor 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 estándar o 443 si se usa un servidor web seguro). Para las comunicaciones del servidor Citrix, el firewall debe permitir el tráfico ICA entrante en los puertos 1494 y 2598.

Si el firewall se ha configurado para la traducción de direcciones de red (NAT), es posible usar la Interfaz Web para definir las asignaciones desde las direcciones internas hacia las direcciones externas y los puertos. Por ejemplo, si el servidor Citrix Virtual Apps and Desktops no se ha configurado con una dirección alternativa, es posible configurar la Interfaz Web para proporcionar una dirección alternativa a la aplicación Citrix Workspace para iOS. A continuación, la aplicación Citrix Workspace para iOS se conecta con el servidor mediante la dirección externa y el número de puerto.

TLS

La aplicación Citrix Workspace para iOS admite el uso de TLS 1.0, 1.1 y 1.2 con los siguientes conjuntos de cifrado para las conexiones TLS con XenApp y XenDesktop:

- TLS_RSA_WITH_AES_256_GCM_SHA384
- TLS_RSA_WITH_AES_128_GCM_SHA256
- TLS_RSA_WITH_AES_256_CBC_SHA
- TLS_RSA_WITH_AES_128_CBC_SHA
- TLS_RSA_WITH_RC4_128_SHA
- TLS_RSA_WITH_RC4_128_MD5

- TLS_RSA_WITH_3DES_EDE_CBC_SHA

> **Nota:**
>
> La aplicación Citrix Workspace para iOS en iOS 9 y versiones posteriores no admite los siguientes conjuntos de cifrado TLS:
>
> - TLS_RSA_WITH_RC4_128_SHA
> - TLS_RSA_WITH_RC4_128_MD5

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. Estas organizaciones pueden exigir también el uso de cifrado validado, como FIPS 140 (Federal Information Processing Standard). FIPS 140 es un estándar para cifrado.

La aplicación Citrix Workspace para iOS 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 iOS usa criptografía de plataforma (iOS) para las conexiones entre la aplicación Citrix Workspace para iOS y StoreFront.

Configurar y habilitar TLS

La configuración de TLS consta de dos pasos:

1. Configure el Traspaso SSL en el servidor de Citrix Virtual Apps and Desktops y en el servidor de la Interfaz Web. 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 usuario

Si quiere usar TLS para proteger las comunicaciones entre las instancias de la aplicación Citrix Workspace para iOS habilitadas con TLS y Citrix Virtual Apps and Desktops, se necesita un certificado raíz en el dispositivo de usuario que pueda verificar la firma de la entidad de certificación en el certificado del servidor.

El sistema iOS incluye aproximadamente 100 certificados raíz comerciales ya instalados, pero, 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, se puede 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 al llavero de iOS.

Para agregar un certificado raíz a las llaves

1. Envíese un correo electrónico con el archivo del certificado.
2. Abra el archivo del certificado en el dispositivo. Esto inicia automáticamente la aplicación Acceso a llaves.
3. Siga las indicaciones para agregar el certificado.
4. A partir de iOS 10, compruebe que el certificado es de confianza desde Ajustes de iOS > Acerca de > Ajustes de confianza de los certificados. En Ajustes de confianza de los certificados, consulte la sección “Activar confianza total en los certificados raíz”. Compruebe que su certificado está seleccionado para la confianza total.

Se instalará el certificado raíz. Los clientes compatibles con TLS y todas las aplicaciones que utilicen TLS podrán usar el certificado raíz.

Sitio de XenApp y XenDesktop

Para configurar el sitio de XenApp y XenDesktop:

> **Importante:**
>
> - Citrix Secure Gateway 3.x se admite en la aplicación Citrix Workspace para iOS mediante sitios de XenApp y XenDesktop.
> - Citrix Secure Gateway 3.x se admite en la aplicación Citrix Workspace para iOS mediante sitios web de Citrix Virtual Apps.
> - Solo se admite la autenticación de un factor en los sitios de XenApp y XenDesktop, y la autenticación de dos factores en los sitios web de Citrix Virtual Apps.
> - Es necesario utilizar la Interfaz Web versión 5.4, que se admite en todos los exploradores web integrados.

Antes de comenzar esta configuración, instale y configure Citrix Gateway para que funcione con la Interfaz Web. Es posible adaptar estas instrucciones para que se adapten a su entorno específico.

Si utiliza una conexión de Citrix Secure Web Gateway, no configure Citrix Gateway en la aplicación Citrix Workspace para iOS.

El software de la aplicación Citrix Workspace para iOS utiliza un sitio de XenApp y XenDesktop para obtener información sobre las aplicaciones a las que un usuario tiene derecho, y las presenta en la aplicación Citrix Workspace para iOS que se ejecuta en el dispositivo. Esto es similar al modo en que se utiliza la Interfaz Web para las conexiones tradicionales de Citrix Virtual Apps basadas en SSL para

las que se puede configurar un dispositivo Citrix Gateway. Los sitios de XenApp y XenDesktop que se ejecutan en la Interfaz Web 5.x contienen esta capacidad de configuración.

Configure el sitio de XenApp y XenDesktop para que admita conexiones desde una conexión de Citrix Secure Gateway:

1. En el sitio de XenApp y XenDesktop, seleccione Manage secure client access > Edit secure client access settings.
2. Cambie el método de acceso a Direct con Gateway.
3. Escriba el FQDN de Secure Web Gateway.
4. Escriba la información de Secure Ticket Authority (STA).

> **Nota:**
>
> Para Citrix Secure Gateway, Citrix recomienda la utilización de la ruta predeterminada de Citrix para este sitio (//NombreServidorXenApp/Citrix/PNAgent). La ruta predeterminada permite que los usuarios especifiquen el FQDN de Secure Web Gateway al que se están conectando, en lugar de la ruta completa al archivo config.xml que reside en el sitio de XenApp y XenDesktop (por ejemplo, //NombreServidorXenApp/RutaPersonalizada/config.xml).

Para configurar Citrix Secure Gateway

1. En Citrix Secure Gateway, use el asistente de configuración de Citrix Secure Gateway para configurar Citrix Secure Gateway de manera que funcione con el servidor en la red segura que aloja el sitio de servicios XenApp. Después de seleccionar la opción Indirecta, introduzca la ruta del FQDN de su servidor Secure Web Gateway y continúe con los pasos del asistente.
2. Pruebe la conexión desde un dispositivo de usuario para asegurarse de que Secure Web Gateway está configurado correctamente para la asignación de certificados y red.

Para configurar el dispositivo móvil

1. Al agregar una cuenta de Citrix Secure Gateway, introduzca el nombre de dominio completo (FQDN) del servidor Secure Gateway en el campo **Dirección**:
   - Si creó el sitio de XenApp y XenDesktop con la ruta predeterminada (/Citrix/PNAgent), escriba el FQDN de Secure Web Gateway: FQDNdeSecureGateway.NombreDeEmpresa.com
   - Si personalizó la ruta del sitio de XenApp y XenDesktop, escriba la ruta completa del archivo config.xml. Por ejemplo: FQDNdeSecureGateway.NombreDeEmpresa.com/RutaPersonalizada
2. Si configura la cuenta manualmente, desactive la opción de Citrix Gateway en el cuadro de diálogo **Nueva cuenta**.

Solución de problemas

August 17, 2020

Sesiones desconectadas

Los usuarios pueden desconectarse (no cerrar la sesión) de una sesión de la aplicación Citrix Workspace para iOS mediante los siguientes métodos:

- Mientras está viendo una aplicación publicada o un escritorio en una sesión:
  - toque la flecha en la parte superior de la pantalla para mostrar el menú desplegable de la sesión.
  - toque el botón **Inicio** para volver a la pantalla de inicio.
  - observe la sobra blanca debajo del icono de una de las aplicaciones publicadas que aún están en una sesión activa: toque el icono.
  - toque Desconectar.
- Cierre la aplicación Citrix Workspace para iOS.
  - haga un doble toque el botón **Inicio** del dispositivo.
  - busque la aplicación Citrix Workspace para iOS en la vista App Switcher iOS.
  - toque Desconectar en el diálogo que aparece.
- Pulsar en el botón de inicio en el dispositivo móvil.
- Tocar Inicio o Cambiar en el menú desplegable de la aplicación.

La sesión permanece en estado desconectado. Si bien el usuario puede reconectarse más tarde, puede asegurarse de que las sesiones desconectadas queden inactivas después de un intervalo específico. Para ello, configure un tiempo de espera de sesión para la conexión ICA-tcp en Configuración de host de sesión de Escritorio remoto (anteriormente “Configuración de servicios de Terminal Server”). Para obtener más información sobre la configuración de Servicios de Escritorio remoto (anteriormente “Servicios de Terminal Server”), consulte la documentación de Microsoft Windows Server.

Contraseñas caducadas

La aplicación Citrix Workspace para iOS admite el cambio de las contraseñas caducadas por parte de los usuarios. Se les solicitará que introduzcan la información requerida.

Dispositivos liberados por jailbreak

Los usuarios pueden poner en peligro la seguridad de la implementación si se conectan con dispositivos iOS liberados por jailbreak. Los dispositivos liberados por jailbreak son aquellos que han sido

modificados por sus usuarios, normalmente para evitar ciertas medidas de protección de la seguridad.

Cuando la aplicación Citrix Workspace para iOS detecta un dispositivo iOS liberado por jailbreak, muestra una alerta al usuario. Para ayudar a proteger mejor la seguridad de su entorno, puede configurar StoreFront o la Interfaz Web para intentar impedir la ejecución de sus aplicaciones desde dispositivos liberados por jailbreak detectados.

Requisitos

- Citrix Receiver para iOS 6.1 o versiones posteriores
- StoreFront 3.0 o Interfaz Web 5.4 o versiones posteriores
- Acceso a StoreFront o a la Interfaz Web con una cuenta de administrador

Para impedir que los dispositivos liberados por jailbreak detectados puedan ejecutar aplicaciones

1. Inicie sesión en el servidor StoreFront o el servidor de Interfaz Web como usuario con privilegios de administrador.
2. Busque el archivo default.ica, que se encuentra en alguna de estas ubicaciones:
    - **C:\inetpub\wwwroot\Citrix***storename***conf** (Microsoft Internet Information Services)
    - **C:\inetpub\wwwroot\Citrix***storename***App_Data** (Microsoft Internet Information Services)
    - **./usr/local/tomcat/webapps/Citrix/XenApp/WEB-INF** (Apache Tomcat)
3. En la sección **[Application]**, agregue: **AllowJailBrokenDevices=OFF**
4. Guarde el archivo y reinicie el servidor StoreFront o el servidor de Interfaz Web.

Una vez reiniciado el servidor StoreFront, los usuarios que vean la alerta sobre dispositivos liberados por jailbreak ya no podrán iniciar aplicaciones desde el servidor StoreFront o el servidor de Interfaz Web.

Para permitir que los dispositivos liberados por jailbreak detectados ejecuten aplicaciones

Si no configura el parámetro AllowJailBrokenDevices, el comportamiento predeterminado es mostrar la alerta a los usuarios de dispositivos liberados por jailbreak, pero permitirles iniciar aplicaciones de todos modos.

Si quiere permitir explícitamente que los usuarios ejecuten aplicaciones desde dispositivos liberados por jailbreak:

1. Inicie sesión en el servidor StoreFront o el servidor de Interfaz Web como usuario con privilegios de administrador.
2. Busque el archivo default.ica, que se encuentra en alguna de estas ubicaciones:
   - **C:\inetpub\wwwroot\Citrix***storename***conf** (Microsoft Internet Information Services)
   - **C:\inetpub\wwwroot\Citrix***storename***App_Data** (Microsoft Internet Information Services)
   - **./usr/local/tomcat/webapps/Citrix/XenApp/WEB-INF** (Apache Tomcat)
3. En la sección **[Application]**, agregue: **AllowJailBrokenDevices=ON**
4. Guarde el archivo y reinicie el servidor StoreFront o el servidor de Interfaz Web.

Cuando el parámetro AllowJailBrokenDevices se ha configurado con el valor ON, los usuarios ven la alerta de uso de dispositivos liberados por jailbreak, pero pueden ejecutar aplicaciones desde StoreFront o la Interfaz Web.

Pérdida de la calidad de sonido HDX

En Citrix Virtual Apps and Desktops, es posible que la calidad del sonido HDX enviado a la aplicación Citrix Workspace para iOS se deteriore al usar sonido y vídeo a la vez. Este problema ocurre cuando las directivas HDX de Citrix Virtual Apps and Desktops no pueden gestionar la cantidad de información de sonido y vídeo. Para obtener información sobre cómo crear directivas para mejorar la calidad de sonido, consulte el artículo CTX123543 de Knowledge Center.

Teclas numéricas y caracteres especiales

Si las teclas numéricas o los caracteres IME chinos no funcionan correctamente, inhabilite la opción de teclado Unicode. Para ello, vaya a **Parámetros** > **Opciones de teclado** y desactive la opción **Usar teclado Unicode**.

Conexiones lentas

Si se perciben conexiones lentas al sitio de XenApp y XenDesktop, o problemas como, por ejemplo, iconos de aplicación que faltan o mensajes del tipo “Error del controlador de protocolo”, como solución, en el servidor Citrix Virtual Apps y Citrix Secure Web Gateway o en el servidor de la Interfaz Web, inhabilite las propiedades del adaptador Citrix PV Ethernet siguientes para la interfaz de red (estas propiedades están habilitadas de forma predeterminada):

- Large Send Offload
- Offload IP Checksum
- Offload TCP Checksum
- Offload UDP Checksum

No se necesita el reinicio del servidor. Esta solución se aplica a Windows Server 2003 y 2008 de 32 bits. Windows Server 2008 R2 no se ve afectado por este problema.

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