



Aplicación Citrix Workspace para Android

Contents

Aplicación Citrix Workspace para Android	2
Acerca de esta versión	2
Funciones en Technical Preview	8
Aplicación Citrix Workspace 22.4.0 para Android: Tech Preview	19
Requisitos previos para la instalación	20
Instalación, actualización	25
Introducción	25
Configurar	29
Configurar la aplicación Citrix Workspace mediante soluciones de administración unificada de dispositivos de punto final	46
Periféricos	59
Prolongar pantalla	66
Experiencia de usuario	69
Experiencia en las sesiones	76
Experiencia en los almacenes	95
Autenticación	96
Protección	99
Solucionar problemas técnicos	102
SDK y API	110
Elementos retirados	111

Aplicación Citrix Workspace para Android

March 22, 2024

La aplicación Citrix Workspace para Android proporciona acceso móvil de tabletas y teléfonos a:

- Escritorios y aplicaciones virtuales
- Aplicaciones táctiles para un uso moderado de tabletas como alternativa a los equipos de escritorio.

El método preferido para instalar o actualizar la aplicación Citrix Workspace para Android es obtenerla de [Google Play](#) mediante un dispositivo Android. Se permiten actualizaciones automáticas cuando hay nuevas versiones disponibles.

Para obtener información sobre las funciones disponibles en la aplicación Citrix Workspace para Android, consulte [Tabla de funciones de la aplicación Citrix Workspace](#).

Para obtener información detallada sobre funciones, problemas resueltos y problemas conocidos, consulte la página [Acerca de esta versión](#).

Para obtener información sobre los elementos retirados, consulte la página [Elementos retirados](#).

Idiomas disponibles

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

Documentación antigua

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

Acerca de esta versión

June 26, 2024

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

Nota:

¿Busca funciones en Technical Preview? Hemos seleccionado una lista para que pueda tenerlas en un solo lugar. Explore nuestra página [Funciones en Technical Preview](#) y comparta sus comentarios mediante el enlace adjunto al formulario de Podio.

Novedades de la versión 24.5.0

Función de autenticación mediante FIDO2 al conectarse a almacenes de la nube

A partir de la versión 24.5.0, los usuarios pueden autenticarse en la aplicación Citrix Workspace mediante la autenticación sin contraseña basada en FIDO2 al conectarse a almacenes de la nube. FIDO2 ofrece un método de autenticación integrado que permite a los empleados de la empresa acceder a aplicaciones y escritorios dentro de sesiones virtuales sin necesidad de introducir un nombre de usuario o una contraseña. Esta función admite tanto itinerancia (solo USB) como autenticadores de plataforma (código PIN, reconocimiento facial y huella digital únicamente). Esta función es compatible con la versión 9 y posteriores de Android.

La autenticación FIDO2 es compatible con las fichas personalizadas de Chrome. Si está interesado en utilizar la autenticación FIDO2 con WebView, registre su interés utilizando el [formulario de Podio](#).

Nota:

Esta función está habilitada de manera predeterminada.

Escáner de documentos

Si ha iniciado sesión en la aplicación Citrix Workspace, puede utilizar la función de escaneo de documentos para escanear muchos documentos y transferirlos a la sesión de escritorio virtual.

Nota:

- Esta función está habilitada de manera predeterminada.

Requisitos previos

- [La asignación de unidades del cliente \(CDM\)](#) debe estar habilitada para el almacén.
- El escáner de documentos requiere acceso de lectura y escritura en el dispositivo. Para habilitar el acceso, siga estos pasos:
 1. Desde su perfil, toque **Parámetros de aplicación** > **Parámetros de almacén**.
 2. Toque su almacén actual.
 3. Toque **Almacenamiento del dispositivo** y, a continuación, seleccione **Acceso total**.

Para obtener más información sobre cómo usar esta función, consulte [Escáner de documentos](#) en la documentación de ayuda.

Anuncio de retirada

A partir de la versión 24.5.0, la aplicación Citrix Workspace para Android no admite las versiones 9, 10 y 11 del sistema operativo Android. Para obtener resultados óptimos, actualice los dispositivos Android con el sistema operativo de Android más reciente.

Para obtener más información, consulte [Elementos retirados](#).

Technical Preview

- [Redirección de audio con micrófonos externos](#).
- [Inicio de sesión único para máquinas virtuales habilitadas con Microsoft Entra ID](#)

Problema solucionado en 24.5.0

No hay problemas resueltos en esta versión.

Problema conocido en la versión 24.5.0

- Al iniciar una sesión de escritorio virtual en un dispositivo compatible con DeX y hacer clic en el botón **Prolongar** de la barra de herramientas de la sesión, la sesión se desconecta y se cierra la ventana de la pantalla extendida.

Este problema se produce en la configuración del monitor externo cuando se utiliza la versión 24.4.0 de la aplicación Citrix Workspace para Android y un dispositivo Samsung Galaxy Tab S9 Ultra con OneUI 6.0. [HDX-65584]

Novedades de la versión 24.4.0

En esta versión, se trató una serie de áreas para mejorar la estabilidad y el rendimiento general.

Anuncio de retirada de los protocolos TLS 1.0 y TLS 1.1

Citrix tiene previsto retirar la compatibilidad con los protocolos TLS 1.0 y TLS 1.1 en futuras versiones. Los protocolos alternativos son TLS 1.2 o TLS 1.3. Para obtener más información, consulte [Elementos retirados](#).

Problemas resueltos en la versión 24.4.0

Los intentos de instalar la versión 24.1.0 de la aplicación Citrix Workspace fallan y se produce un error de incompatibilidad. Este problema se produce en algunos dispositivos de Zebra que no tienen cámara. [CVADHELP-24843]

Problemas conocidos en la versión 24.4.0

No hay nuevos problemas conocidos.

Nota:

Para obtener una lista completa de los problemas de las versiones anteriores, consulte la sección [Problemas conocidos](#).

Versiones anteriores

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

24.3.5

Novedades

Esta versión incluye mejoras en la recopilación de registros. El archivo de registros ahora contiene información más completa que puede ayudar a los administradores de TI y a los equipos de Asistencia al cliente a analizar mejor cada caso.

Enviar la configuración de la aplicación Citrix Workspace a través de UEM Anteriormente, podía configurar la URL de almacén en la aplicación Citrix Workspace.

A partir de esta versión, puede configurar los parámetros de la aplicación Citrix Workspace en los dispositivos administrados mediante cualquier herramienta de administración unificada de dispositivos de punto final (UEM) que se implemente en su infraestructura.

Nota:

Como administrador, si tiene la opción de configurar los parámetros de la aplicación Citrix Workspace mediante UEM y el Global App Configuration Service (GACS), donde UEM siempre tendrá prioridad sobre GACS.

Para obtener más información sobre la configuración, consulte [Enviar la configuración de la aplicación Citrix Workspace a través de UEM](#).

Problemas resueltos

No hay problemas resueltos en esta versión.

24.3.0

Novedades

Función para autenticación biométrica tras inactividad Una vez que caduca el temporizador de inactividad, se le pide al usuario final que se autentique mediante funciones biométricas como el reconocimiento facial y el escaneo de huellas digitales.

La forma más fiable de autenticación biométrica disponible para el usuario final depende del OEM de su dispositivo y se le pedirá usarla como corresponda en cada caso.

Para obtener más información sobre la configuración del temporizador de inactividad, consulte [Tiempo de espera por inactividad en sesiones de la aplicación Citrix Workspace](#).

Problemas resueltos

No hay problemas resueltos en esta versión.

Problemas conocidos

Problemas conocidos en la versión 22.6.5

- Al abrir una aplicación web o una aplicación SaaS, los botones y puntos suspensivos de la barra de tareas no funcionan como es debido. El problema se produce después de activar la **Interfaz Web** en la pantalla **Agregar cuenta**. [RFANDROID-10263]

Problemas conocidos en la versión 21.4.0

No se han observado nuevos problemas conocidos en esta versión.

Nota:

Al inscribirse en el perfil de trabajo de la aplicación Citrix Workspace, no se pueden iniciar sesiones con el explorador Chrome desde un archivo ICA del perfil personal. Sin embargo, el prob-

El error no se produce con Citrix Secure Web al agregar la URL del archivo ICA a la lista de exclusión.

Problemas conocidos en la versión 20.3.0

En un dispositivo Samsung DeX, es posible que no pueda cancelar la redirección del dispositivo USB si cierra la solicitud de permiso sin tocar el botón **Cancelar**. [RFANDROID-5397]

Problemas conocidos en la versión 20.2.0

Los intentos de reconexión fallan tras tocar **Conectar** en el cuadro de diálogo **Reconexión automática de clientes**. El problema se produce en sesiones conectadas a Citrix XenApp y XenDesktop 7.6 CU 8. [RFANDROID-5151]

Limitaciones

Al iniciar aplicaciones web y SaaS desde la aplicación Citrix Workspace, si la aplicación usa el IdP de Google y requiere que el usuario final inicie sesión, la autenticación falla y se mostrará el mensaje de error “Acceso denegado”.

Technical Preview

Las Technical Previews 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 funciones en Technical Preview, pero agradece los comentarios para mejorarlas. Citrix puede o no actuar a partir de los comentarios en función de su gravedad e importancia.

Avisos legales de terceros

Los productos de Citrix a menudo incluyen código de terceros que da licencia a Citrix para su uso y redistribución, bajo una licencia de código abierto (Open Source). Para informar mejor a sus clientes, Citrix publica el código abierto incluido en los productos Citrix en una lista de código con licencia Open Source.

Para obtener más información acerca del código de licencia Open Source consulte [Open Source Licensed Code](#).

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

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

Elementos retirados

Para obtener información sobre los elementos retirados, consulte la página [Elementos retirados](#).

Documentación antigua

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

Funciones en Technical Preview

June 27, 2024

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

Lista de funciones en Technical Preview

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

Título	Disponible a partir de la versión	Formulario de habilitación (haga clic en el icono)	Formulario de comentarios (haga clic en el icono)
Inicio de sesión único para máquinas virtuales habilitadas con Microsoft Entra ID	24.5.0		
Redirección de audio con micrófonos externos	24.5.0		

Título	Disponible a partir de la versión	Formulario de habilitación (haga clic en el icono)	Formulario de comentarios (haga clic en el icono)
Compatibilidad con audio adaptable	23.11.0		
Compatibilidad con aplicaciones para compartir sesiones multiventana en Samsung DeX	2307		
Ventana de sesión independiente de la aplicación Citrix Workspace para Samsung DeX	23.9.0		
Agregar muchos almacenes mediante UEM	23.8.0		
Modo de imagen incrustada	23.3.5		
Compatibilidad con experiencia mejorada de Single Sign-On (SSO) para aplicaciones web y SaaS	22.3.5		

Inicio de sesión único para máquinas virtuales habilitadas con Microsoft Entra ID

A partir de la versión 24.5.0, la aplicación Citrix Workspace para Android permite a los usuarios iniciar sesión en dispositivos VM unidos a Azure AD mediante la autenticación de inicio de sesión único. En el primer inicio de máquinas virtuales (VM) unidas a Azure AD en la aplicación Citrix Workspace, se solicita a los usuarios que introduzcan las credenciales de la cuenta de Azure para la autenticación.

Los siguientes inicios de sesión de VDA se realizan automáticamente sin solicitar credenciales hasta que caduque el token de autenticación.

Notas:

- Esta función solo se aplica a los almacenes de la nube unidos a Azure AD.
- De forma predeterminada, esta función está inhabilitada. Esta función se halla en una versión Tech Preview únicamente accesible mediante solicitud. Para habilitarla en su entorno, complete el [formulario de Podio](#).
- Puede enviar sus comentarios sobre esta Technical Preview a través del [formulario de Podio](#).

Redirección de audio con micrófonos externos

Esta función se encuentra en una Technical Preview de la versión 24.5.0.

Anteriormente, solo podía usar un dispositivo de sonido en la sesión. A partir de la versión 24.5.0, la aplicación Citrix Workspace para Android muestra todos los dispositivos de sonido locales disponibles en una sesión con sus nombres. Además, también se admiten dispositivos de sonido plug-and-play.

Notas:

- De forma predeterminada, esta función está inhabilitada. Esta función se halla en una versión Tech Preview únicamente accesible mediante solicitud. Para habilitarla en su entorno, complete el [formulario de Podio](#).
- Puede enviar sus comentarios sobre esta Technical Preview a través del [formulario de Podio](#).

Compatibilidad con audio adaptable

Esta función se encuentra en una Technical Preview de la versión 23.11.0.

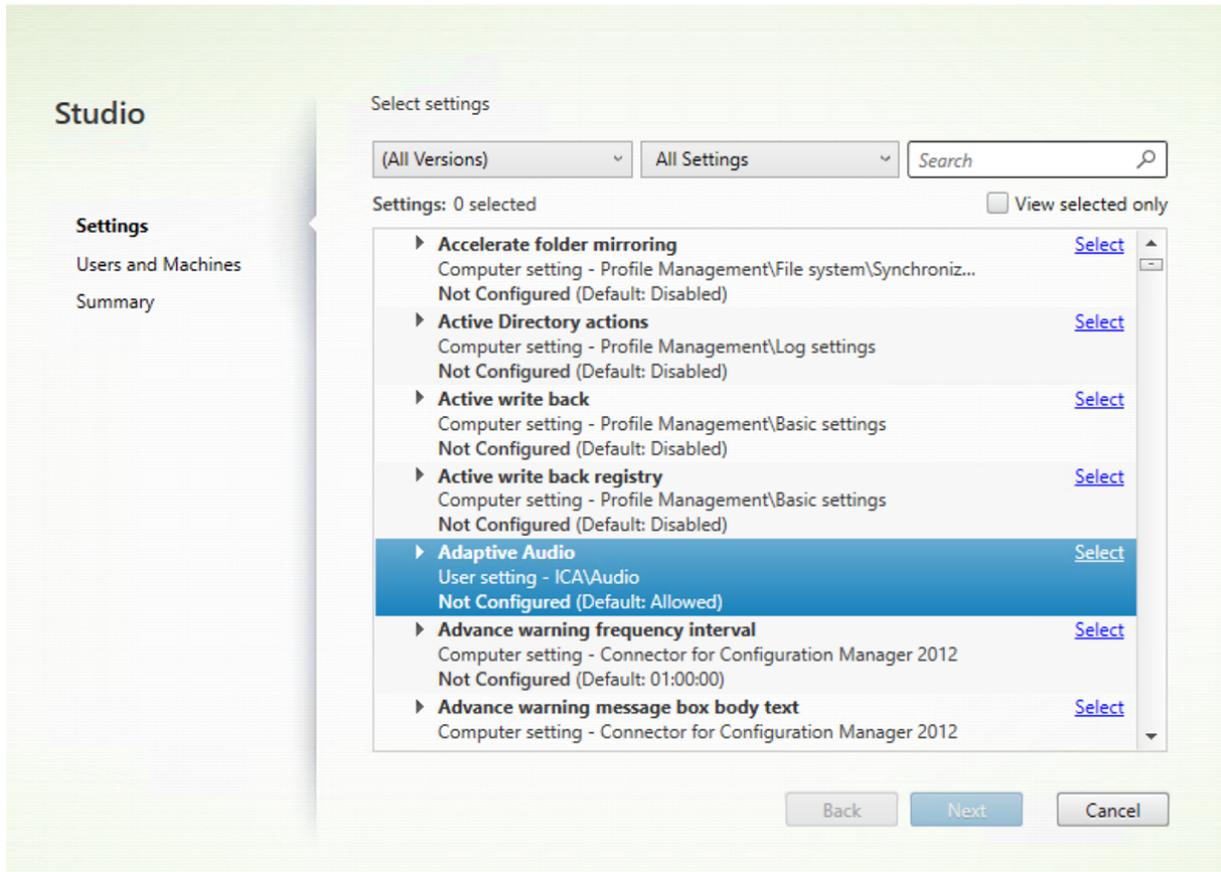
La aplicación Citrix Workspace para Android admite el audio adaptable HDX. Esta función está diseñada para ofrecer a los usuarios una calidad de audio excepcional y una baja latencia.

Notas:

- Esta función se halla en una versión Tech Preview únicamente accesible mediante solicitud. Para habilitarla en su entorno, complete el [formulario de Podio](#).
- Puede enviar sus comentarios sobre esta Technical Preview a través del [formulario de Podio](#).

Puede configurar esta función habilitando la directiva **Audio adaptable**.

Create Policy



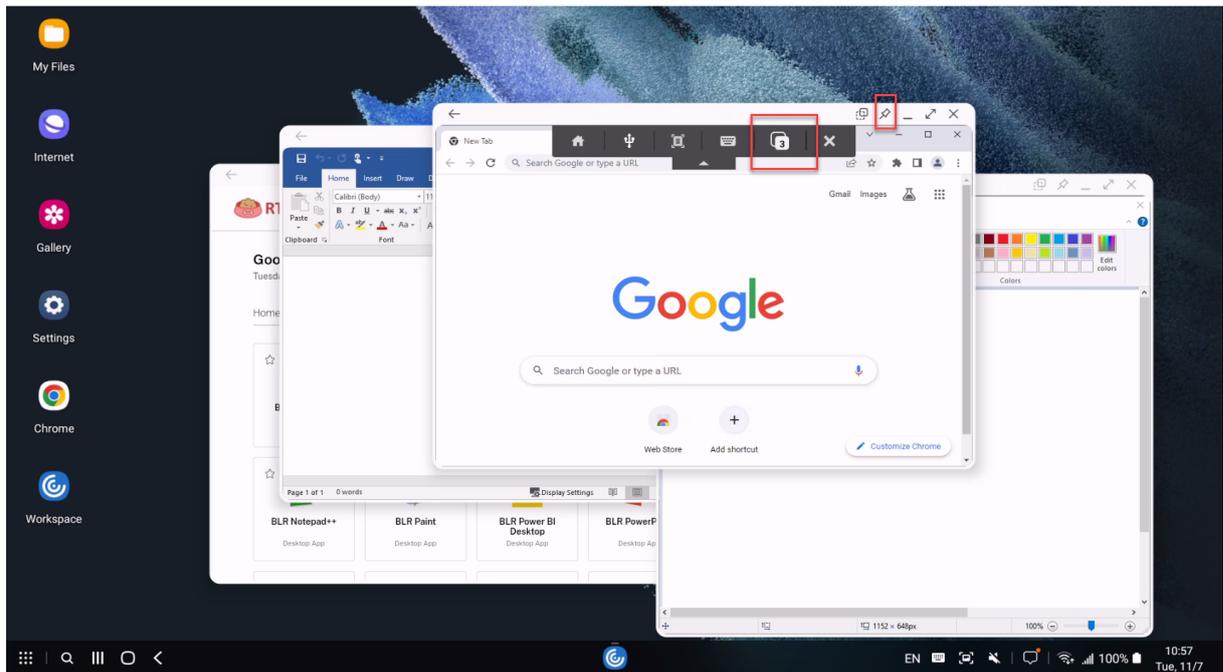
Para obtener más información, consulte el artículo sobre [configuración de la directiva de audio](#) en la documentación de Citrix Virtual Apps and Desktops.

Compatibilidad con aplicaciones para compartir sesiones multiventana en Samsung DeX

Esta función se encuentra en una Technical Preview de la versión 23.11.0.

La versión 23.9.5 de la aplicación Citrix Workspace introdujo una ventana de sesión independiente para que los usuarios finales tuvieran una experiencia similar a la de un escritorio. Sin embargo, solo se admitía una ventana de sesión.

A partir de la versión 23.11.0, la aplicación Citrix Workspace admite funcionalidad multitarea y ofrece a los usuarios una experiencia similar a la de un escritorio. Permite abrir varias aplicaciones en la misma sesión para que se ejecuten simultáneamente. Estas aplicaciones se abren en ventanas independientes.



Por ejemplo, al abrir la aplicación Citrix Workspace e iniciar el explorador Google Chrome, Microsoft Paint y Microsoft Word, las tres aplicaciones se abren en ventanas independientes. Para ver la cantidad de ventanas abiertas y cambiar a la ventana de otra aplicación en la sesión, utilice el icono de **cambio de aplicación** de la barra de herramientas de la sesión.

Notas:

- Esta función se halla en una versión Tech Preview únicamente accesible mediante solicitud. Para habilitarla en su entorno, complete el [formulario de Podio](#).
- Puede enviar sus comentarios sobre esta Technical Preview a través del [formulario de Podio](#).
- La primera aplicación que inicie puede tardar un minuto en iniciar sesión y cargar su perfil de usuario.

Caso de uso

Al abrir algunas aplicaciones en la pantalla DeX, aún puede abrir aplicaciones desde la aplicación Citrix Workspace instalada en su dispositivo móvil. Cuando inicie una sesión de aplicación en la pantalla de su dispositivo móvil, aparecerá un cuadro de diálogo para cerrar la sesión existente en DeX. En el dispositivo móvil, la aplicación se abre en modo de ventana única.

Si hace clic en el icono de la aplicación Citrix Workspace en la pantalla DeX cuando se abre una ventana de aplicación en la pantalla del dispositivo, pero la aplicación está en modo de ventana única, debe salir del modo de ventana de sesión de la aplicación en la pantalla DeX y, a continuación, volver a abrir la aplicación para acceder al modo de sesión multiventana.

Puede realizar lo siguiente:

- Haga clic en el botón de anclar en la esquina superior derecha de la ventana para anclar la aplicación de ventana. La ventana anclada permanece siempre visible.
- Acceda al botón de la barra de herramientas de la sesión en todas las ventanas de aplicación.
- Minimice, maximice, mueva y cierre la ventana de aplicación.
- Cambie de aplicación y multitarea haciendo clic con el mouse, haciendo doble clic, arrastrando y pulsando el teclado.

Limitaciones de la función

- El título de la ventana de vista previa de la barra de tareas de Samsung DeX muestra **Workspace** en lugar del nombre real de la aplicación.
- No se admite el cambio de tamaño de la ventana orientada al servidor. En otras palabras, si el tamaño de la ventana del lado del servidor está establecido o limitado, las solicitudes para cambiar el tamaño desde el lado del cliente no funcionan. Esta configuración provoca una discrepancia entre los gráficos de la ventana local y remota.
- La ventana del lado del cliente tiene un tamaño de ventana mínimo. En otras palabras, el tamaño mínimo de una ventana en una pantalla DeX con una resolución de 1920x1080 es de 220x220 con la barra de título, y el tamaño de rectángulo disponible es de 220x189.
- Es posible que algunas opciones del menú se extiendan y aparezcan fuera del límite de la aplicación principal. Es posible que las opciones del menú ampliado aparezcan en las otras ventanas de aplicación.
- La imagen de vista previa de una aplicación en la barra de tareas puede superponerse y cubrir la vista previa de otra aplicación.

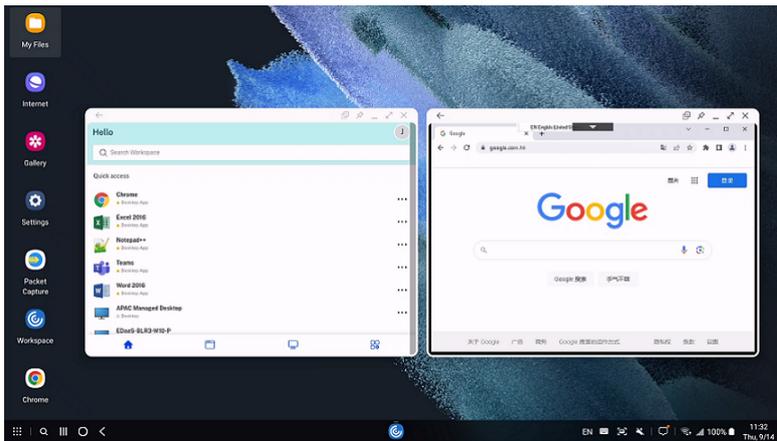
Ventana de sesión independiente de la aplicación Citrix Workspace para Samsung DeX

Esta función se encuentra en una versión preliminar técnica de la versión 23.9.5.

Antes, cuando iniciaba una sesión de escritorio o aplicación virtual, se abría en la ventana de la interfaz de usuario de la aplicación Citrix Workspace. Con esta disposición, los usuarios finales tenían que tocar el icono de **inicio** de la barra de herramientas de la sesión y desconectar la sesión para acceder a otra aplicación o escritorio desde la aplicación Citrix Workspace. El modo de ventana única afectaba negativamente a la experiencia de usuario con el escritorio en los dispositivos Samsung DeX.

A partir de la versión 23.9.5, la aplicación Citrix Workspace presenta una ventana de sesión independiente que hace que la multitarea sea más eficiente y fácil de usar. Con esta función, puede disfrutar de una experiencia similar a la de un escritorio.

Por ejemplo, al abrir el explorador Google Chrome, se abre en una ventana independiente, como se muestra en la siguiente captura de pantalla.



Limitaciones conocidas de la función

Solo se admite una ventana de sesión. En otras palabras, la ventana de sesión existente se cierra al abrir una nueva ventana de sesión.

Notas:

- Esta función se halla en una versión Tech Preview únicamente accesible mediante solicitud. Para habilitarla en su entorno, complete el [formulario de Podio](#).
- Puede enviar sus comentarios sobre esta Technical Preview a través del [formulario de Podio](#).

Agregar muchos almacenes mediante UEM

Esta función se encuentra en una Technical Preview de la versión 23.8.0.

Ahora, los administradores pueden usar soluciones de administración unificada de dispositivos de punto final (Unified Endpoint Management o UEM) con el fin de configurar muchos almacenes para dispositivos Android administrados.

Nota:

- Puede enviar sus comentarios sobre esta Technical Preview a través del formulario de [Podio](#).

Los detalles de cada almacén se pueden agregar a un archivo JSON. A continuación, este archivo JSON se puede cargar mientras se configura la directiva de configuración de aplicaciones. Los detalles incluyen:

- URL del almacén
- tipo de almacén (opcional)

Nota:

- Si no se proporciona el tipo de almacén, la interfaz predeterminada se considera nativa.

- nombre del almacén (opcional)

Nota:

- UEM admite un almacén de la nube y muchos almacenes locales.

El archivo JSON debe estar en formato clave-valor. Para obtener más información, consulte estos datos de JSON de ejemplo:

Nota:

- Los datos de JSON de ejemplo están relacionados con Microsoft Intune. Es posible que los datos de JSON varíen para otras soluciones de UEM.

```
1 {
2
3   "kind": "androidenterprise#managedConfiguration",
4   "productId": "app:com.citrix.Receiver",
5   "managedProperty": [
6     {
7
8       "key": "stores",
9       "valueBundleArray": [
10        {
11
12          "managedProperty": [
13            {
14
15              "key": "url",
16              "valueString": "test.cloud.com"
17            }
18          ],
19          "key": "url",
20          "valueString": "test.cloud.com"
21        },
22        {
23          "key": "storeType",
24          "valueInteger": 1
25        },
26        {
27          "key": "displayName",
28          "valueString": "1"
29        }
30      ]
31    }
32  ]
33 }
```

```

32     }
33   ,
34     {
35       "managedProperty": [
36         {
37           "key": "url",
38           "valueString": "test2.cloud.com"
39         },
40         {
41           "key": "storeType",
42           "valueInteger": 2
43         },
44         {
45           "key": "displayName",
46           "valueString": "2"
47         }
48       ]
49     },
50     {
51       "key": "restrict_user_store_modification",
52       "valueBool": false
53     }
54   ]
55 }
56 ]
57 }
58 ]
59 }
60 ,
61 {
62   "key": "restrict_user_store_modification",
63   "valueBool": false
64 }
65 ]
66 }
67 ]
68 }
69 }
70 <!--NeedCopy-->

```

Notas:

- (predeterminado) Si el valor entero se establece en 1, los usuarios pueden ver la carga nativa o predeterminada del almacén.
- Si el valor entero se establece en 2, los usuarios pueden ver el almacén dentro de una interfaz web.

Para cargar el archivo JSON que contiene las configuraciones del almacén, seleccione **Enter JSON data** en la lista desplegable **Configuration settings format**.

Home > Apps | App configuration policies >

Create app configuration policy

✔ Basics ✔ **Settings** ③ Assignments ④ Review + create

Permissions
Permissions granted here will override the "Default app permissions" policy for the selected apps.
[Learn more about Android runtime permissions](#)

+Add
Not configured

Configuration Settings
Configuration settings format ⓘ

Download JSON template

1

Connected apps
Enable users to connect this app across the work and personal profiles ⓘ Enabled Not configured

This setting only works for personally-owned and corporate-owned work profile

Modo de imagen incrustada

Esta función se encuentra en una Technical Preview de la versión 23.3.5.

La aplicación Citrix Workspace para Android admite el modo de imagen incrustada (PiP), lo que le permite reducir el tamaño de las sesiones de escritorio, las aplicaciones SaaS o las aplicaciones web a ventanas flotantes. Puede mover esta ventana libremente por la pantalla y colocarla en cualquier lugar. El modo PiP libera la pantalla de inicio de la aplicación Citrix Workspace para que pueda completar otras tareas.

Para usar esta función:

- En la sesión de escritorio, toque el botón **Inicio** de la barra de herramientas de la sesión.

o

- Mientras usa una aplicación SaaS o web, toque el **menú de puntos suspensivos (...)** > **Minimizar**.

Toque la ventana flotante para ver la aplicación en pantalla completa y ciérrala con el icono **X** de la ventana flotante. La ventana flotante aparece automáticamente en pantalla completa al minimizar otra aplicación.

Nota:

- Esta función se halla en una versión Tech Preview únicamente accesible mediante solicitud. Para habilitarla en su entorno, complete el [formulario de Podio](#).

La función PiP es compatible con las implementaciones locales y de la nube. Sin embargo, para las implementaciones en la nube, puede:

- Minimizar las aplicaciones web en una ventana PiP.
- Cambiar entre una sesión de escritorio y una aplicación web tocando la ventana flotante.

Nota:

Solo puede mantener dos aplicaciones activas a la vez. Una en modo de pantalla completa y la otra minimizada como imagen incrustada:

- 2 aplicaciones web o SaaS
- 1 aplicación web o SaaS y 1 sesión de escritorio o aplicación virtual

Compatibilidad con experiencia mejorada de Single Sign-On (SSO) para aplicaciones web y SaaS

Esta función se encuentra en una Technical Preview de la versión 22.3.5.

Esta función simplifica la configuración de SSO para aplicaciones web y SaaS internas al usar proveedores de identidades (IdP) de terceros.

La experiencia mejorada de SSO reduce todo el proceso a unos pocos comandos. Elimina el requisito previo obligatorio de configurar Citrix Secure Private Access en la cadena de IdP para configurar SSO. También mejora la experiencia del usuario, siempre que se utilice el mismo IdP para la autenticación tanto en la aplicación Workspace como en la aplicación web o SaaS correspondiente que se inicie.

Puede registrarse para obtener esta versión Technical Preview a través de este [formulario de Podio](#).

De la versión Technical Preview a la versión de disponibilidad general (GA)

Nombres de funcionalidad	Versión de disponibilidad general
Equiparación de PPP	24.1.0
Enviar la configuración de la aplicación Citrix Workspace a través de UEM	24.3.5
Escáner de documentos	24.5.0

Aplicación Citrix Workspace 22.4.0 para Android: Tech Preview

April 21, 2022

Novedades

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

Problemas resueltos

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

Problemas conocidos

No se han observado nuevos problemas conocidos en esta versión.

Recomendaciones y notas

- La aplicación Citrix Workspace para Android 22.4.0 admite Android 12.
- Si se halla en almacenes HTTP, para obtener un contexto protegido, le recomendamos pasar a almacenes HTTPS. Para obtener más información, consulte [HTTPS](#).

Requisitos previos para la instalación

June 26, 2024

Requisitos del sistema y compatibilidad

Requisitos de dispositivo

La aplicación Citrix Workspace es compatible con la versión 12 de Android y versiones posteriores.

Para obtener resultados óptimos, actualice los dispositivos Android con el sistema operativo de Android más reciente.

Puede iniciar sesiones de la aplicación Citrix Workspace desde Workspace para Web cuando el explorador web es compatible con Workspace para Web. Si no puede iniciar sesiones, configure su cuenta directamente a través de la aplicación Citrix Workspace.

Importante:

Si tiene instalada una versión Technical Preview de la aplicación Citrix Workspace para Android, desinstálela antes de instalar la nueva versión.

Requisitos del servidor

StoreFront:

- StoreFront 2.6 o versiones posteriores

Ofrece acceso directo a almacenes de StoreFront. La aplicación Citrix Workspace para Android también admite versiones anteriores de StoreFront.

- StoreFront configurado con Workspace para sitios web

Ofrece acceso a los almacenes de StoreFront a través de un explorador web. Para conocer las limitaciones de esta implementación, consulte la documentación de StoreFront.

Habilite las directivas de reescritura proporcionadas por Citrix Gateway.

Citrix Virtual Apps and Desktops (cualquiera de los siguientes productos):

- Citrix Virtual Apps 7.5 o posterior
- Citrix Virtual Apps and Desktops 7.x o posterior

Conexiones y certificados

La aplicación Citrix Workspace admite conexiones HTTP, HTTPS e ICA sobre TLS con un servidor de Citrix Virtual Apps and Desktops mediante cualquiera de las configuraciones siguientes.

Para conexiones LAN:

- StoreFront 2.6 o versiones posteriores
- Sitio de servicios XenApp (antes llamado Agente de Program Neighborhood).

Para conexiones remotas seguras (cualquiera de los productos siguientes):

- Citrix Gateway 12.1 y versiones posteriores (incluidas las versiones [VPX](#), [MPX](#) y [SDX](#)).

Certificados TLS

Al proteger las conexiones remotas mediante TLS, el dispositivo móvil hace lo siguiente:

1. Autentica el certificado TLS de la puerta de enlace remota en un almacén local de entidades de certificación raíz de confianza.
2. Reconoce automáticamente los certificados emitidos comercialmente (como Verisign y Thawte) siempre que exista el certificado raíz para la entidad de certificación en el almacén local.

Certificados privados (firmados automáticamente)

Al instalar un certificado privado en la puerta de enlace remota, asegúrese de que el certificado raíz de la entidad de certificación de la organización esté instalado en el dispositivo de usuario. Esta configuración le ayuda a acceder correctamente a los recursos de Citrix mediante la aplicación Citrix Workspace para Android.

Nota:

Cuando no puede verificar el certificado de la puerta de enlace al conectarse, como el certificado raíz no está incluido en el almacén de claves local, aparece una advertencia sobre certificados que no son de confianza. Si un usuario opta por ignorar la advertencia, se muestra una lista de aplicaciones. Sin embargo, las aplicaciones no se inician.

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 Android admite certificados comodín.

Certificados intermedios y Citrix Gateway

Si la cadena de certificados incluye un certificado intermedio, deberá agregar este certificado al certificado del servidor de Citrix Gateway. Consulte el artículo en Knowledge Center correspondiente a su edición de Citrix Gateway: [CTX114146](#) y [CTX124937](#)

Directiva de validación conjunta de certificados de servidor

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

Importante:

Antes de instalar la aplicación Citrix Workspace para Android, confirme que los certificados presentes en el servidor o en Citrix Gateway se han configurado correctamente como se describe aquí. Las conexiones pueden fallar si:

- la configuración del servidor o de Citrix Gateway incluye un certificado raíz incorrecto.
- la configuración del servidor o de Citrix Gateway no incluye todos los certificados intermedios.
- la configuración del servidor o de Citrix Gateway incluye un certificado intermedio caducado o no válido.
- la configuración del servidor o de Citrix Gateway incluye un certificado intermedio con firmas cruzadas.

Cuando valida un certificado de servidor, la aplicación Citrix Workspace para Android usa ahora **todos** los certificados suministrados por el servidor (o por Citrix Gateway) para validarlo. A continuación, también verifica si 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 Citrix Gateway) debe estar configurado con el conjunto correcto de certificados. Un conjunto incorrecto de certificados puede provocar que falle la conexión de la aplicación Citrix Workspace para Android.

Supongamos que se configura un dispositivo Citrix Gateway con estos certificados válidos. Se recomienda para clientes que requieran una validación más estricta. Pueden aplicar una validación más estricta al determinar exactamente qué certificado raíz utiliza la aplicación Citrix Workspace para Android:

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

- “Ejemplo de certificado raíz”

A continuación, la aplicación Citrix Workspace para Android verifica si todos estos certificados son válidos. La aplicación Citrix Workspace para Android también verifica si ya confía en un “Certificado raíz de ejemplo”. Si la aplicación Citrix Workspace para Android no confía en “Certificado raíz de ejemplo”, la conexión falla.

Importante

Algunas entidades de certificación tienen más de un certificado raíz. Si necesita usar esta validación más estricta, compruebe que la configuración usa el certificado raíz correspondiente. Por ejemplo, actualmente hay dos certificados (“DigiCert”/ “GTE CyberTrust Global Root” y “DigiCert Baltimore Root”/ “Baltimore CyberTrust Root”) que pueden validar los mismos certificados de servidor.

En algunos dispositivos de usuario, están disponibles ambos certificados raíz. En otros dispositivos, solo uno está disponible (“DigiCert Baltimore Root”/ “Baltimore CyberTrust Root”). Si configura “GTE CyberTrust Global Root” en la puerta de enlace, fallan las conexiones de la aplicación Citrix Workspace para Android en esos dispositivos de usuario. Consulte la documentación de la entidad de certificación para determinar qué certificado raíz puede usarse. Tenga en cuenta que los certificados raíz también caducan, como todos los demás certificados.

Nota:

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

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

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

La aplicación Citrix Workspace para Android usará esos dos certificados. Luego, busca un certificado raíz en el dispositivo del usuario. Si encuentra uno que se valida correctamente y también es de confianza (por ejemplo, “Ejemplo de certificado raíz”), la conexión se realiza correctamente. De lo contrario, la conexión falla. Tenga en cuenta que esta configuración proporciona el certificado intermedio que necesita la aplicación Citrix Workspace para Android, pero también permite que la aplicación Citrix Workspace para Android elija cualquier certificado raíz válido y de confianza.

Supongamos ahora que se configura una Citrix Gateway con estos certificados:

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

La aplicación Citrix Workspace para Android lee el certificado raíz incorrecto y la conexión falla.

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

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

Algunas entidades de certificación usan un certificado intermedio con firmas cruzadas. Está pensado para situaciones donde haya más de un certificado raíz y

un certificado raíz anterior se use al mismo tiempo que un certificado raíz posterior. En este caso, hay al menos dos certificados intermedios. Por ejemplo, el certificado raíz anterior “Class 3 Public Primary Certification Authority” tiene el certificado intermedio correspondiente de firmas cruzadas “Verisign Class 3 Public Primary Certification Authority - G5”.

No obstante, un certificado raíz posterior correspondiente “Verisign Class 3 Public Primary Certification Authority - G5” también está disponible y reemplaza a “Class 3 Public Primary Certification Authority”. El certificado raíz posterior no usa ningún certificado intermedio con firmas cruzadas.

El certificado intermedio con firmas cruzadas y el certificado raíz tienen el mismo nombre de sujeto (Emitido para). Sin embargo, el certificado intermedio con firmas cruzadas tiene otro nombre de emisor (Emitido por). Distingue el certificado intermedio con firmas cruzadas de un certificado intermedio normal (como el “Ejemplo de certificado intermedio 2”).

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

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

No configure Citrix Gateway para que use el certificado intermedio con firmas cruzadas, porque seleccionará el certificado raíz anterior:

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

No se recomienda configurar Citrix Gateway solamente con el certificado del servidor:

- “Ejemplo de certificado de servidor”

Cuando la aplicación Citrix Workspace para Android no puede localizar todos los certificados intermedios, la conexión falla.

Instalación, actualización

June 21, 2023

Actualizaciones

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

- Actualice la versión de su aplicación Citrix Workspace mediante [Google Play](#).
- Descargue la aplicación Citrix Workspace de la página de [descargas de Citrix](#) e instale la aplicación para actualizar la aplicación Citrix Receiver a la aplicación Citrix Workspace.

Para obtener información sobre las funciones disponibles en la aplicación Citrix Workspace para Android, consulte [Tabla de funciones de la aplicación Citrix Workspace](#).

Para acceder a la documentación de Citrix Receiver para Android, consulte [Citrix Receiver](#).

Introducción

March 22, 2024

Cuenta

Para crear una cuenta, haga lo siguiente:

1. Introduzca una URL de almacén válida o su dirección de correo electrónico en el campo **Dirección**. Por ejemplo, storefront.organización.com. Rellene los demás campos con los detalles necesarios.
2. Introduzca las credenciales de usuario.

Acceder a StoreFront a través de Citrix Gateway

Para obtener información sobre cómo configurar el acceso a StoreFront a través de Citrix Gateway, consulte:

- [Configurar y administrar almacenes](#)
- [Integración de StoreFront con Citrix Gateway](#)

Detección de cuentas basada en direcciones de correo electrónico

Puede configurar la aplicación Citrix Workspace 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 Android.

La aplicación Citrix Workspace para Android determina el dispositivo Citrix Gateway o el servidor de StoreFront asociados a la dirección de correo electrónico en función de los registros de servicios (SRV) del Sistema de nombres de dominio (DNS). A continuación, se solicita al usuario que inicie sesión para acceder a sus aplicaciones, escritorios y datos alojados.

Archivo de aprovisionamiento

Puede utilizar StoreFront para crear archivos de aprovisionamiento que tengan los detalles de conexión de las cuentas. Puede poner estos archivos a disposición de los usuarios para que puedan configurar la aplicación Citrix Workspace para Android de forma automática.

Después de instalar la aplicación Citrix Workspace para Android, los usuarios solo tienen que abrir el archivo **CR** en el dispositivo para configurar la aplicación Citrix Workspace para Android. Si configura Workspace para sitios web, los usuarios también pueden obtener los archivos de aprovisionamiento de la aplicación Citrix Workspace para Android desde esos sitios.

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

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

Cuando proporcione a los usuarios los detalles de las cuentas que deben introducir manualmente, asegúrese de incluir la siguiente información. La siguiente información permite a los usuarios conectarse correctamente a sus escritorios alojados:

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

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

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

Conceder acceso a Citrix Virtual Apps and Desktops y Citrix DaaS

La aplicación Citrix Workspace necesita la configuración de StoreFront para entregar aplicaciones, archivos y escritorios desde una implementación de Citrix Virtual Apps and Desktops o Citrix DaaS (antes denominado Citrix Virtual Apps and Desktops Service).

StoreFront

Puede configurar StoreFront para que proporcione servicios de autenticación y entrega de recursos para la aplicación Citrix Workspace, lo que le permite crear almacenes de empresa centralizados para entregar:

- Escritorios y aplicaciones a través de Citrix Virtual Apps and Desktops o Citrix DaaS.
- XenMobile Apps y aplicaciones móviles que ha preparado para su organización a través de XenMobile.

La autenticación entre la aplicación Citrix Workspace y un almacén de StoreFront se puede gestionar de varias formas:

- Los usuarios dentro del firewall pueden conectarse directamente a StoreFront.
- Los usuarios fuera del firewall pueden conectarse a StoreFront a través de Citrix Gateway.
- Los usuarios fuera del firewall pueden conectar a través de Citrix Gateway con StoreFront.

Conexión con StoreFront La aplicación Citrix Workspace para Android permite iniciar sesiones desde Workspace para Web, siempre que el explorador web que se utilice sea compatible con Workspace para Web. Si no puede iniciar sesiones, configure su cuenta a través de la aplicación Citrix Workspace para Android directamente.

Sugerencia

Cuando se usa Workspace para Web desde un explorador web, las sesiones no se inician automáticamente al descargar un archivo **ICA**. El archivo **ICA** debe abrirse manualmente justo después de descargarlo para que la sesión se inicie.

Con StoreFront, los almacenes que se crean consisten en servicios que proporcionan una infraestructura de recursos y autenticación para la aplicación Citrix Workspace. Cree almacenes que cuenten y agreguen escritorios y aplicaciones desde los sitios de XenDesktop y XenApp para, así, habilitar estos recursos para los usuarios.

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 Android.

Configure los almacenes para StoreFront tal como configura Citrix Virtual Apps and Desktops y Citrix DaaS. No se requiere ninguna configuración especial para los dispositivos móviles.

Conectarse a través de Citrix Gateway

La aplicación Citrix Workspace para Android es compatible con Citrix Gateway 11 y versiones posteriores para acceder a:

- Sitios de XenApp y XenDesktop
- Almacenes de StoreFront 2.6, 3.0, 3.5, 3.6, 3.7, 3.8, 3.9 y 3.11

Puede crear varias directivas de sesión en el mismo servidor virtual en función de lo siguiente:

- El tipo de conexión (como ICA, VPN sin cliente o VPN)
- El tipo de implementación de Workspace (Workspace para Web o aplicación Citrix Workspace instalada localmente)

Las directivas pueden crearse desde un único servidor virtual.

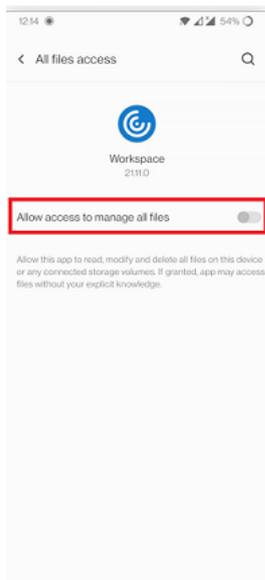
Cuando los usuarios crean cuentas en la aplicación Citrix Workspace, deben introducir su dirección de correo electrónico o el FQDN correspondiente de su servidor de Citrix Gateway. Por ejemplo, si no se puede establecer la conexión cuando se utiliza la ruta predeterminada, introduzca la ruta completa al servidor de Citrix Gateway.

Funcionalidad VPN

Puede acceder a la web interna, a aplicaciones de software como servicio (SaaS) y a sitios web alojados por su empresa, independientemente de la ubicación de su acceso. Puede acceder a estos recursos, alojados por su empresa, sin conexión VPN. Esta función solo está disponible para clientes de almacenes en la nube.

Permitir el acceso para administrar todos los archivos

Presentamos la opción de permiso: **Permitir el acceso para administrar todos los archivos**. Le recomendamos que habilite este permiso para obtener un rendimiento óptimo. Sus archivos permanecen protegidos.



Configurar

May 17, 2024

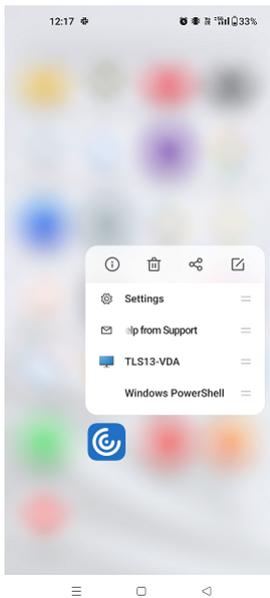
Acceso al micrófono para cada almacén

La función de confianza en clientes selectivos permite a la aplicación Citrix Workspace confiar en el acceso desde una sesión de VDA. Puede conceder acceso a unidades cliente y dispositivos de hardware locales, como micrófonos y cámaras web.

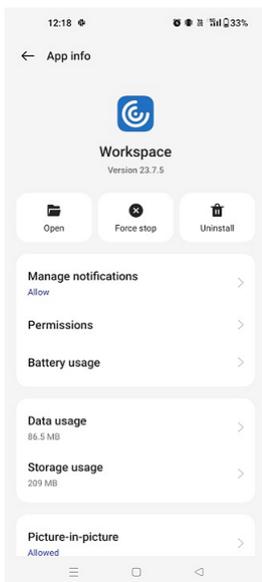
Antes, la configuración del acceso al micrófono se aplicaba en todos los almacenes configurados.

Para acceder al micrófono, ahora la aplicación Citrix Workspace requiere el permiso del usuario final para cada almacén. Proporcione el permiso para acceder al micrófono de esta manera:

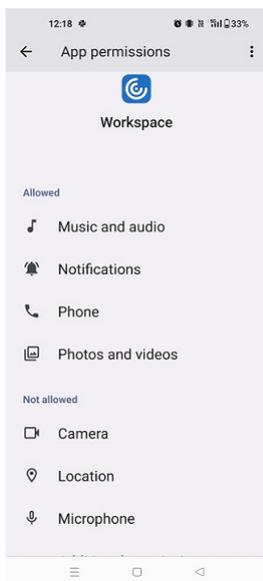
1. Mantenga pulsado el icono de la aplicación Citrix Workspace y toque el icono de **información de la aplicación** ⓘ .



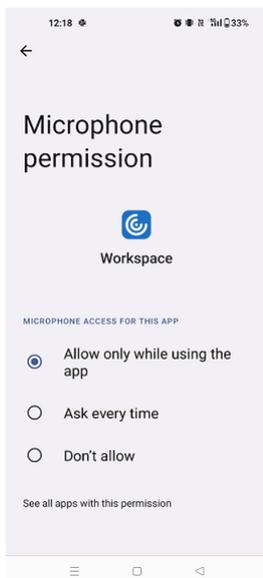
2. Toque **Permisos**.



3. Toque **Microphone**.



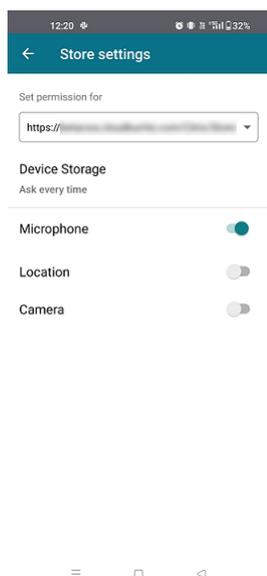
4. Seleccione **Permitir solo si la aplicación está en uso**.



Ahora puede acceder al micrófono mientras usa la aplicación Citrix Workspace.

Configure los niveles de acceso de la siguiente manera:

1. Abra la aplicación Citrix Workspace y seleccione **Parámetros > Parámetros de almacén**.
2. En la opción **Establecer permisos para**, seleccione un almacén en el menú desplegable.



3. Habilite **Micrófono**.

Ahora, el micrófono está habilitado, y puede usarlo mientras usa la aplicación Citrix Workspace en su dispositivo Android.

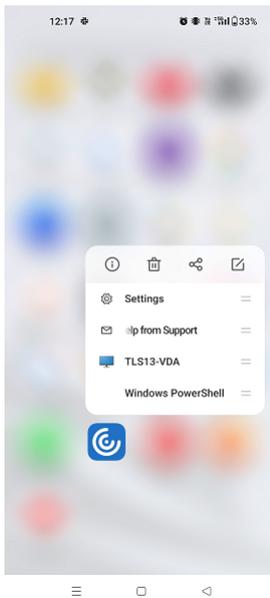
Acceso a la ubicación para cada almacén

La función de confianza en clientes selectivos permite a la aplicación Citrix Workspace confiar en el acceso desde una sesión de VDA.

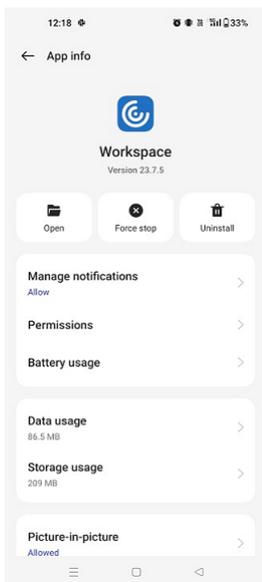
Antes, la configuración del acceso a la ubicación se aplicaba en todos los almacenes configurados.

Para acceder a la ubicación, a partir de la versión 21.3.0, la aplicación Citrix Workspace requiere el permiso del usuario final para cada almacén. Proporcione el permiso del usuario para acceder a la ubicación de esta manera:

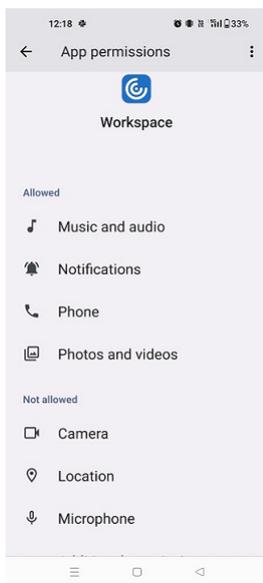
1. Mantenga pulsado el icono de la aplicación Citrix Workspace y toque el icono de **información de la aplicación** ⓘ .



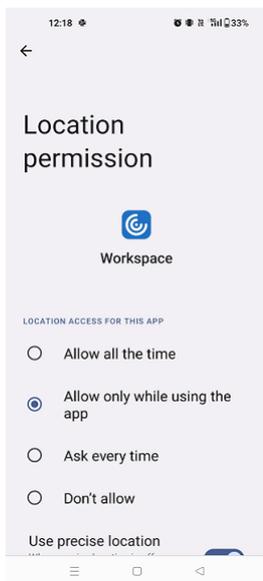
2. Toque **Permisos**.



3. Toque **Location**.



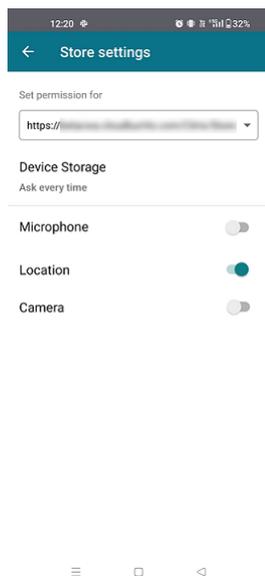
4. Seleccione **Permitir solo si la aplicación está en uso**.



Ahora puede acceder a la ubicación mientras usa la aplicación Citrix Workspace.

Configure los niveles de acceso de la siguiente manera:

1. Abra la aplicación Citrix Workspace y seleccione **Parámetros > Parámetros de almacén**.
2. En la opción **Establecer permisos para**, seleccione un almacén en el menú desplegable.



3. Habilite **Ubicación**.

Ahora, la ubicación está habilitada, y puede usarla mientras usa la aplicación Citrix Workspace en su dispositivo Android.

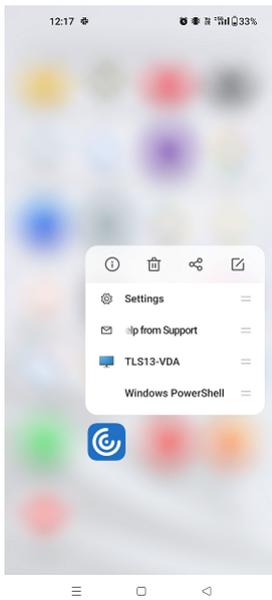
Acceso a la cámara para cada almacén

La función de confianza en clientes selectivos permite a la aplicación Citrix Workspace confiar en el acceso desde una sesión de VDA. Puede conceder acceso a unidades cliente y dispositivos de hardware locales, como micrófonos y cámaras web.

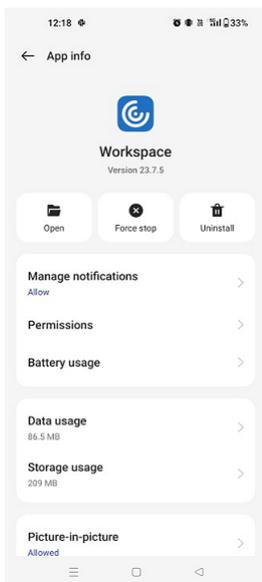
Antes, la configuración del acceso a la cámara se aplicaba en todos los almacenes configurados.

Para acceder a la cámara del teléfono, ahora la aplicación Citrix Workspace requiere el permiso del usuario final para cada almacén. Proporcione el permiso para acceder a la cámara de esta manera:

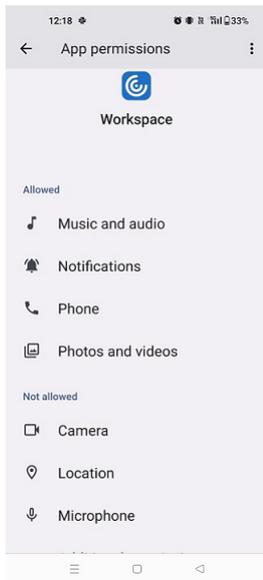
1. Mantenga pulsado el icono de la aplicación Citrix Workspace y toque el icono de **información de la aplicación** ⓘ .



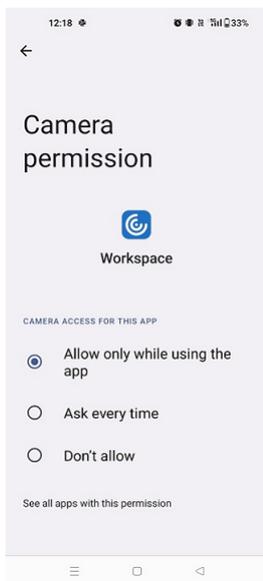
2. Toque **Permisos**.



3. Toque **Camera**.



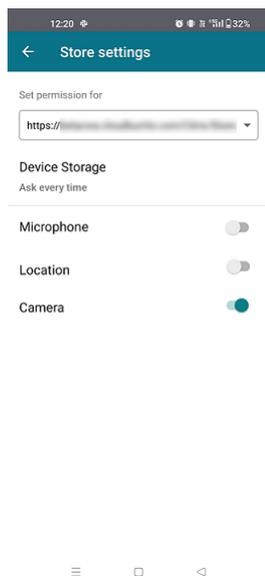
4. Seleccione **Permitir solo si la aplicación está en uso**.



Ahora puede acceder a la cámara mientras usa la aplicación Citrix Workspace.

Configure los niveles de acceso de la siguiente manera:

1. Abra la aplicación Citrix Workspace y seleccione **Parámetros > Parámetros de almacén**.
2. En la opción **Establecer permisos para**, seleccione un almacén en el menú desplegable.



3. Habilite la **cámara**.

Ahora, la cámara está habilitada, y puede usarla mientras usa la aplicación Citrix Workspace en su dispositivo Android.

Administrar marcas de función

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

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

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

Permitir el tráfico a las siguientes URL

- events.launchdarkly.com
- stream.launchdarkly.com
- clientstream.launchdarkly.com
- Firehose.launchdarkly.com
- mobile.launchdarkly.com
- app.launchdarkly.com

Incluir direcciones IP en una lista de permitidos

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

Requisitos del sistema para LaunchDarkly

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

- Servicio de LaunchDarkly.
- Servicio de escucha de APNs

Disposición para inhabilitar el servicio de LaunchDarkly

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

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

```
1      {
2
3          "assignedTo": [
4              "AllUsersNoAuthentication"
5          ],
6          "category": "Third Party Services",
7          "settings": [
8              {
9
10                 "name": "Enable Launch Darkly",
11                 "value": "true"
12             }
13         ],
14         "userOverride": false
15     }
16
17
18
19 <!--NeedCopy-->
```

Para obtener más información, consulte la documentación de [Global App Configuration Service](#).

En la implementación local, haga lo siguiente:

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

Por ejemplo, `<account id=... name="Store">`. Antes de la etiqueta `</account>`, vaya a las propiedades de esa cuenta de usuario:

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

3. Agregue la etiqueta **enableLaunchDarkly** y establezca el valor como **false**.

```
<property name="enableLaunchDarkly" value="false"/>
```

Nota:

La mayoría de las funciones están detrás de una marca de función y LaunchDarkly las controla. En los entornos en los que está inhabilitada, debe esperar un mínimo de 90 días para poder usar la función.

Asociación de tipos de archivos

Como requisito previo para que funcione esta función, vaya a los parámetros de la aplicación Citrix Workspace para Android y configure la opción **Usar almacenamiento del dispositivo** en **Acceso total**. También está disponible, como opción adicional, **Preguntar siempre** para que se le solicite permiso antes de acceder al almacenamiento de su dispositivo en una sesión.

Nota:

La opción **Preguntar siempre** es un parámetro que se aplica a cada sesión. No se traslada a la siguiente sesión.

Al seleccionar **Preguntar siempre**, cualquier acceso a su dispositivo generado por el sistema podría provocar la aparición de la ventana **Usar almacenamiento del dispositivo** (por ejemplo, en el cierre de sesión), lo que es de esperar.

La aplicación Citrix Workspace para Android lee y aplica los parámetros configurados por los administradores en Citrix Studio.

Para aplicar la asociación de tipos de archivo (File Type Association o FTA) en una sesión, asegúrese de que los usuarios finales se conecten al servidor del almacén donde está configurada la asociación de tipos de archivo.

En el dispositivo del usuario, seleccione el archivo que quiere iniciar en el Explorador de archivos y toque **Abrir**. El sistema operativo Android ofrece una opción para iniciar el archivo mediante la aplicación Citrix Workspace para Android (al aplicar la asociación de tipos de archivo configurada por el administrador) o una aplicación diferente. En función de lo que haya seleccionado, puede haber o no una aplicación predeterminada. Puede cambiar la aplicación predeterminada mediante la opción para cambiar el valor predeterminado.

Nota:

Esta función solo está disponible en StoreFront y requiere la versión 7 de Citrix Virtual Apps and Desktops o una posterior.

Problemas y limitaciones conocidos de la función

1. Es posible que la autenticación con tarjeta inteligente sea más lenta que la autenticación mediante contraseña. Por ejemplo, después de desconectarse de una sesión, espere aproximadamente 30 segundos antes de volver a conectarse. Si se vuelve a conectarse a una sesión desconectada demasiado rápido, esto puede hacer que la aplicación Citrix Workspace se bloquee.
2. La autenticación mediante tarjeta inteligente no se admite en las comunidades.
3. Es posible que algunos usuarios tengan un número PIN global para tarjetas inteligentes. Sin embargo, cuando los usuarios inician sesión con una cuenta de tarjeta inteligente, deben introducir el PIN de PIV y no el PIN de tarjeta inteligente global, lo cual es una limitación de terceros.
4. Citrix recomienda que salga y reinicie la sesión de la aplicación Citrix Workspace después de cerrar la sesión de la cuenta de la tarjeta inteligente.
5. No se admite el uso de varias tarjetas inteligentes USB.
6. Puede acceder solo a los formatos de archivo MIME admitidos por Microsoft Office, Adobe Acrobat Reader y Bloc de notas mediante la función de asociación de tipos de archivo.

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

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

Información adicional

Citrix gestiona sus datos de acuerdo con las condiciones de su contrato con Citrix. Sus datos están protegidos como se especifica en [Citrix Services Security Exhibit](#). Este documento está disponible en el [Centro de confianza de Citrix](#).

Puede inhabilitar el envío de datos de CEIP a Citrix y a Google Analytics para Firebase (excepto los dos elementos de datos recopilados para Google Analytics para Firebase que se indican mediante un * en la tabla siguiente):

1. Inicie la aplicación Citrix Workspace y seleccione **Parámetros**.
2. Seleccione **Preferencias avanzadas**.
Se mostrará el cuadro de diálogo **Preferencias avanzadas**.
3. Desmarque la opción **Enviar estadísticas de uso**.

Nota:

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

Elementos concretos de datos CEIP recopilados por Google Analytics para Firebase:

Versión del sistema operativo*	Versión de la aplicación Workspace*	Configuración de la autenticación	Información de dispositivos
--------------------------------	-------------------------------------	-----------------------------------	-----------------------------

Método de inicio de sesiones	Tipo de almacén de Citrix	Configuración de la asignación de unidades del cliente	
Información de la sesión	Uso de <code>Receiverconfig.txt</code>	Configuración de la redirección de USB	Información de usuario de HDX RTME
Configuración de las conexiones HTTP y HTTPS	Información del protocolo de conexiones ICA	Acción de revisión de la aplicación Workspace	Inhabilitar la configuración de Firebase
Cantidad de almacenes agregados	Acción de captura de pantalla	Acciones de usuario de la función RSA	Cantidad de usuarios de StoreFront y de la aplicación Workspace
Acción de actualización de aplicaciones	Actualización del sistema operativo	Acción de visualización de pantalla	Eliminación de aplicaciones
Conexiones de vista web	Borrado de datos de aplicación	Ejecución de aplicaciones	Inicio de sesión de la aplicación

Migración de una cuenta local a una cuenta de la nube

Los administradores pueden migrar fácilmente a los usuarios finales de una URL de almacén de StoreFront local a una URL de Workspace. Los administradores pueden realizar la migración con una interacción mínima del usuario final mediante [Global App Configuration Service](#).

Para llevar a cabo la configuración:

1. Vaya a la URL de [Global App Configuration Store Settings API](#) e introduzca la URL del almacén de la nube.
Por ejemplo, `https://discovery.cem.cloud.us/ads/root/url/<hash coded store URL>/product/workspace/os/ios`.
2. Vaya **API Exploration > SettingsController > postDiscoveryApiUsingPOST** y toque **POST**.
3. Toque **INVOKE API**.
4. Introduzca y cargue los detalles de la carga útil. Introduzca la fecha de caducidad del almacén de StoreFront en la marca de tiempo de epoch en milisegundos.

Por ejemplo,

```
1 "migrationUrl": [
```

```
2 {
3
4
5 "url": "<cloud store url>"
6 "storeFrontValidUntil": "<epoch timestamp in milliseconds>",
7 }
8
9 ] ,
10 <!--NeedCopy-->
```

5. Toque **EJECUTAR** para activar el servicio.

Experiencia del usuario final para esta función

Como usuario final, si utiliza la aplicación Citrix Workspace por primera vez, después de una autenticación correcta, aparece la pantalla de migración **Presentación del nuevo Citrix Workspace** (si cumple los requisitos). Después de tocar la opción **Probar el nuevo Citrix Workspace**, comienza la migración. Si la migración se realiza correctamente, puede acceder al almacén de Workspace (almacén de la nube).

Nota:

Puede omitir la migración tres veces. Luego, la migración se aplica sin que se pueda omitir.



Después de migrar al almacén (de la nube) de Workspace, puede ver tanto el almacén de StoreFront como el almacén de Workspace en **Parámetros**. Cuando cambia de un almacén de la nube al almacén local de StoreFront, aparece una pantalla de comentarios para recopilar su respuesta.

Nota:

El almacén de StoreFront tiene fecha de caducidad. Una vez transcurrida la fecha de caducidad,

el almacén se elimina.

Uso de la versión más reciente

Esta función le ayuda a usar la versión más reciente de la aplicación Citrix Workspace. Cuando los usuarios finales utilizan una versión de la aplicación Citrix Workspace inferior a la versión de Playstore, el mensaje integrado de la aplicación pide a los usuarios que se actualicen a la versión más reciente.

Al tocar **Update**, la actualización se produce en segundo plano y puede seguir usando la aplicación. Puede ver el progreso en la snackbar. Una vez finalizada la descarga, aparece este cuadro de diálogo:

Toque **Relaunch now** para usar la versión más reciente. Si toca **Do it later**, el mensaje para reiniciar la aplicación aparece en el siguiente inicio de la aplicación.

Compatibilidad con canales de Global App Configuration Service

A partir de la versión 23.4.5, los administradores pueden usar Global App Configuration Service para definir parámetros y probarlos antes de implementar la configuración para todos los usuarios finales. Este proceso garantiza una prueba minuciosa de las funciones y funcionalidades antes de cambiar a un entorno de producción.

Nota:

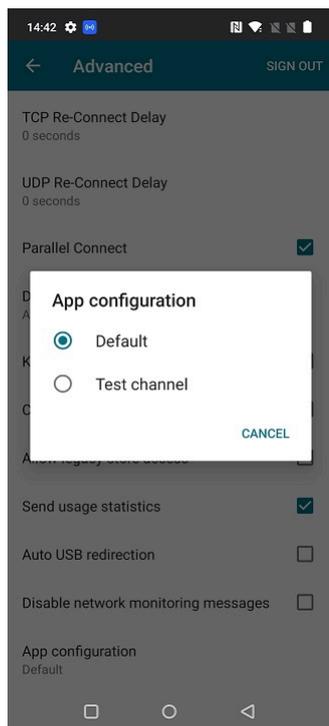
- La aplicación Citrix Workspace para Android admite las configuraciones **Predeterminado** y **Canal de prueba**. De forma predeterminada, todos los usuarios están en el canal **Predeterminado**.

Para obtener más información, consulte la documentación de [Global App Configuration Service](#).

Cómo utilizar esta función

Para probar las configuraciones:

1. En la aplicación Citrix Workspace, vaya a **Parámetros > Avanzados > Configuración de aplicaciones**
2. Seleccione **Canal de prueba**.



Ahora puede iniciar la prueba.

Nota:

- Asegúrese de que las configuraciones de aplicación están presentes en el **canal de prueba**. Para obtener asistencia, contacte con el administrador de su organización.

Configurar la aplicación Citrix Workspace mediante soluciones de administración unificada de dispositivos de punto final

April 18, 2024

Función para configurar almacenes mediante soluciones de administración unificada de dispositivos de punto final

Ahora, la aplicación Citrix Workspace para Android permite la configuración remota de la URL del almacén de Workspace mediante soluciones de administración unificada de dispositivos de punto final. Como administrador, puede administrar las URL de los almacenes de forma remota con pares de clave-valor basados en AppConfig mediante soluciones de administración unificada de dispositivos de punto final.

Para configurar la URL del almacén de Workspace mediante soluciones de administración unificada de dispositivos de punto final, siga estos pasos:

Configurar un almacén mediante soluciones de administración unificada de dispositivos de punto final

La aplicación Citrix Workspace para Android permite la configuración remota de la URL del almacén de Workspace mediante soluciones de administración unificada de dispositivos de punto final.

Para configurar de forma remota la URL del almacén de Workspace mediante soluciones de administración unificada de dispositivos de punto final, siga estos pasos:

1. Inicie sesión en su proveedor de soluciones de administración unificada de dispositivos de punto final.
2. Cree una directiva de configuración de aplicaciones para su aplicación.
3. Agregue el par de clave y valor a la lista de propiedades JSON y rellene estos valores:
 - **clave:** URL
 - **tipo de valor:** cadena
 - **valor:** La URL de su almacén (por ejemplo, prodcwa.cloud.com)

Nota:

- A modo de demostración, en este ejemplo se utiliza Microsoft Intune como la solución de administración unificada de dispositivos de punto final. La interfaz de usuario que se muestra varía según el proveedor de soluciones de administración unificada de dispositivos de punto final.

Settings [Edit](#)

Configuration key	Value type	Configuration value
url	String	prodcwa.cloud.com

Limitaciones

- Si ya hay un almacén de la nube configurado y el administrador configura otro almacén de la nube, se eliminarán el almacén de la nube existente y los datos o parámetros asociados. Recibirá una notificación para informarle de la eliminación en Citrix Workspace. A continuación, debe iniciar sesión de nuevo para agregar el nuevo almacén de la nube a Citrix Workspace.
- Para aplicar nuevas configuraciones, debe cerrar y abrir la aplicación Citrix Workspace.

Función para configurar el tipo de almacén

A partir de la versión 23.6.0, la aplicación Citrix Workspace para Android permite configurar el tipo de almacén mediante el par de clave-valor basado en AppConfig para configurar la aplicación Citrix Workspace. Ahora, los administradores pueden controlar la apariencia de la aplicación.

Este es el par de clave-valor:

- **Clave:** storeType
- **Tipo de valor:** Entero
- **valor:**
 - ☒ Si se establece en 1 (predeterminado), los usuarios pueden ver la carga nativa o predeterminada del almacén.
 - ☒ Si se establece en 2, los usuarios pueden ver el almacén dentro de una interfaz web.

Nota:

Esta función no requiere habilitación.

Controlar las configuraciones de almacén mediante soluciones de administración unificada de dispositivos de punto final

La aplicación Citrix Workspace para Android comenzó a admitir la configuración remota de la URL de almacén de Workspace mediante soluciones de administración unificada de dispositivos de punto final a partir de la versión 23.4.5. Como administrador, puede administrar las URL de los almacenes de forma remota con pares de clave-valor basados en AppConfig mediante soluciones de administración unificada de dispositivos de punto final.

Para obtener más información, consulte [Función para configurar almacenes mediante soluciones de administración unificada de dispositivos de punto final](#).

A partir de la versión 23.7.5, los administradores pueden configurar si los usuarios finales pueden modificar las URL de almacén mediante un par clave-valor basado en AppConfig:

- **clave:** restrict_user_store_modification
- **tipo de valor:** booleano
- **valor:**
 - ☒ Si se establece en **true**, los usuarios finales no pueden modificar el almacén (agregar, eliminar o modificar).
 - ☒ Si se establece en **false**, los usuarios finales pueden modificar el almacén.

Nota:

Si el indicador **restrict_user_store_modification** se establece en **true**, todos los almacenes existentes se eliminan antes de agregar un nuevo almacén configurado para administración unificada de dispositivos de punto final.

Detección y prevención de capturas de pantalla mediante soluciones de administración unificada de dispositivos de punto final (UEM)

A partir de la versión 23.10.0, los administradores pueden impedir que los usuarios finales realicen capturas de pantalla en el nivel de la aplicación Citrix Workspace. Esta función evita las filtraciones de información confidencial o privada. Los administradores pueden configurar esta función mediante un par clave-valor basado en AppConfig:

- clave: restrictScreenshot
- tipo de valor: booleano
- valor:
 - ◇ Si se establece en true, los usuarios finales no podrán realizar capturas de pantalla.
 - ◇ Si se establece en false, los usuarios finales podrán realizar capturas de pantalla.

Enviar la configuración de la aplicación Citrix Workspace a través de UEM

Anteriormente, podía configurar la URL de almacén en la aplicación Citrix Workspace.

A partir de esta versión, puede configurar los parámetros de la aplicación Citrix Workspace en los dispositivos administrados mediante cualquier herramienta de administración unificada de dispositivos de punto final (UEM) que se implemente en su infraestructura.

Nota:

Como administrador, si tiene la opción de configurar los parámetros de la aplicación Citrix Workspace mediante UEM y el Global App Configuration Service (GACS), donde UEM siempre tendrá prioridad sobre GACS.

Configuraciones

Los siguientes datos JSON son un ejemplo de MS Intune que muestra cómo configurar esta función.

```
1 {  
2  
3     "kind": "androidenterprise#managedConfiguration",
```

```

4     "productId": "app:com.citrix.Receiver",
5     "managedProperty": [
6         {
7
8             "key": "stores",
9             "valueBundleArray": [
10                {
11
12                    "managedProperty": [
13                        {
14
15                            "key": "url",
16                            "valueString": ""
17                        },
18                    ,
19                    {
20
21                        "key": "storeType",
22                        "valueInteger": 1
23                    },
24                    ,
25                    {
26
27                        "key": "displayName",
28                        "valueString": ""
29                    }
30                ]
31            }
32        ]
33    },
34    {
35        "key": "url",
36        "valueString": "prodcwa.cloud.com"
37    },
38    {
39        "key": "storeType",
40        "valueInteger": 1
41    },
42    {
43        "key": "displayName",
44        "valueString": ""
45    },
46    {
47
48
49
50
51
52
53
54
55
56

```

```

57     "key": "restrict_user_store_modification",
58     "valueBool": false
59   }
60   ,
61   {
62
63     "key": "restrictScreenshot",
64     "valueBool": true
65   }
66   ,
67   {
68
69     "key": "appSettings",
70     "valueBundleArray": [
71       {
72
73         "managedProperty": [
74           {
75
76             "key": "name",
77             "valueString": ""
78           }
79         ,
80           {
81
82             "key": "value",
83             "valueString": ""
84           }
85         ,
86           {
87
88             "key": "userOverride",
89             "valueBool": false
90           }
91         ]
92       }
93     ]
94   }
95 ]
96 }
97
98 ]
99 }
100
101
102 <!--NeedCopy-->

```

Tabla de pares clave-valor

La siguiente tabla proporciona la información del par clave-valor:

Parámetro	Descripción	Clave	Valor	Tipo de valor	Valor predefinido
Audio	Permite a los usuarios controlar la conexión de audio y micrófono dentro de la aplicación o el escritorio.	audioRecordingSettingsKey	Reproducir y grabar	Cadena	Reproducir y grabar
Texto predictivo	Habilita las sugerencias de texto mientras el usuario escribe.	predictiveText	FALSE	Booleano	FALSE
Teclado extendido	Habilita la compatibilidad con el teclado extendido en una sesión.	showExtendedKeyboard	TRUE	Booleano	TRUE
Redirección de USB genérico	Permite la redirección automática de dispositivos USB arbitrarios desde el dispositivo cliente al VDA.	autoUSB	TRUE	Booleano	FALSE

Parámetro	Descripción	Clave	Valor	Tipo de valor	Valor predefinido
Confirmación de usuario de desconexión de sesión (preguntar antes de salir)	Abre un cuadro de diálogo de confirmación que permite al usuario confirmar antes de desconectar una sesión.	askBeforeExiting	TRUE	Booleano	TRUE
Redirección del portapapeles (Portapapeles)	Permite al usuario utilizar operaciones del portapapeles, como cortar, copiar y pegar en una sesión.	clipboardAccess	TRUE	Booleano	FALSE
Transporte adaptable (EDT)	Habilita Enlightened Data Transport como protocolo preferido, en lugar de TCP, para optimizar el transporte de datos.	edtSetting	TRUE	Booleano	TRUE

Parámetro	Descripción	Clave	Valor	Tipo de valor	Valor predefinido
Orientación de pantalla	Permite a los usuarios seleccionar la orientación de la pantalla en función de la posición del dispositivo.	displayOrientationKey	horizontal	Cadena	Automático
Mantener pantalla activa	Mantiene la pantalla activa y encendida.	keepScreenOnKey	TRUE	Booleano	FALSE
Validación estricta de certificados	Aplica un control más estricto en la validación de los certificados del servidor.	strictCertificateValidation	TRUE	Booleano	FALSE
Acceso al almacén antiguo	Permite a los usuarios acceder a versiones anteriores del almacén.	allowLegacySystemAccess	TRUE	Booleano	FALSE
RealTime Media Engine	Permite realizar llamadas de audio y vídeo de alta definición.	RTMEAccess	TRUE	Booleano	FALSE

Parámetro	Descripción	Clave	Valor	Tipo de valor	Valor predefinido
Redirección USB automática	Permite la redirección automática de dispositivos USB arbitrarios desde el dispositivo cliente al VDA.	autoUSB	TRUE	Booleano	FALSE
Mensajes de supervisión de red	Inhabilita los mensajes de alerta que proporcionan detalles sobre el rendimiento de la red.	DisableChannelMetrics	FALSE	Booleano	FALSE
Teclas extendidas	Accesos directos que se usarán en el teclado de la sesión.	key_map	[“strAltTab”, “strAlt”, “strBackspace”, “strAltF4”]	MultiList	nulo
LaunchDarkly	Habilita el indicador de LaunchDarkly en las funciones de la aplicación Citrix Workspace.	enableLaunchDarkly	TRUE	Booleano	TRUE

A continuación, se muestra un ejemplo de datos JSON. Aquí, el ejemplo muestra diferentes valores de configuración, como:

- Booleano
- Número entero
- Cadena

- Lista de cadenas

```
1 {
2
3   "kind": "androidenterprise#managedConfiguration",
4   "productId": "app:com.citrix.Receiver",
5   "managedProperty": [
6     {
7
8       "key": "stores",
9       "valueBundleArray": [
10        {
11
12          "managedProperty": [
13            {
14
15              "key": "url",
16              "valueString": ""
17            },
18            ,
19            {
20
21              "key": "storeType",
22              "valueInteger": 1
23            },
24            ,
25            {
26
27              "key": "displayName",
28              "valueString": ""
29            }
30          ]
31        }
32      ]
33    },
34    {
35
36      "key": "url",
37      "valueString": "your_store_url"
38    },
39    {
40
41      "key": "storeType",
42      "valueInteger": 1
43    },
44    {
45
46      "key": "displayName",
```

```
52     "valueString": ""
53   }
54   ,
55   {
56
57     "key": "restrict_user_store_modification",
58     "valueBool": false
59   }
60   ,
61   {
62
63     "key": "restrictScreenshot",
64     "valueBool": true
65   }
66   ,
67   {
68
69     "key": "appSettings",
70     "valueBundleArray": [
71       {
72
73         "managedProperty": [
74           {
75
76             "key": "name",
77             "valueString": "showExtendedKeyboard"
78           }
79         ,
80           {
81
82             "key": "value",
83             "valueString": "false"
84           }
85         ,
86           {
87
88             "key": "userOverride",
89             "valueBool": false
90           }
91         ]
92       }
93     ]
94   ,
95   {
96
97     "managedProperty": [
98       {
99
100        "key": "name",
101        "valueString": "enterRegion"
102      }
103    ,
104    {
```

```

105
106         "key": "value",
107         "valueString": "-40"
108     }
109     ,
110     {
111
112         "key": "userOverride",
113         "valueBool": false
114     }
115 ]
116 ]
117 }
118 ,
119 {
120
121     "managedProperty": [
122     {
123
124         "key": "name",
125         "valueString": "displayOrientationKey"
126     }
127     ,
128     {
129
130         "key": "value",
131         "valueString": "Landscape mode"
132     }
133     ,
134     {
135
136         "key": "userOverride",
137         "valueBool": false
138     }
139 ]
140 ]
141 }
142 ,
143 {
144
145     "managedProperty": [
146     {
147
148         "key": "name",
149         "valueString": "askBeforeExiting"
150     }
151     ,
152     {
153
154         "key": "value",
155         "valueString": "true"
156     }
157     ,

```

```
158         {
159             "key": "userOverride",
160             "valueBool": false
161         }
162     ]
163 }
164 ]
165 }
166 ,
167 {
168     "managedProperty": [
169         {
170             "key": "name",
171             "valueString": "key_map"
172         },
173         {
174             "key": "value",
175             "valueString": "['strAltTab','strAlt','strBackspace','strAltF4']"
176         },
177         {
178             "key": "userOverride",
179             "valueBool": true
180         }
181     ]
182 }
183 ]
184 }
185 ]
186 }
187 ]
188 }
189 ]
190 }
191 ]
192 }
193 ]
194 }
195 }
196 }
197 <!--NeedCopy-->
```

Periféricos

May 17, 2024

Modo de entrada Scancode para teclado externo

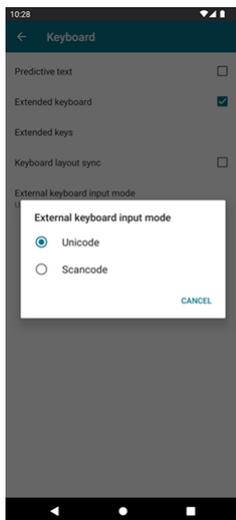
A partir de la versión 24.1.0, puede seleccionar Scancode como modo de entrada del teclado mientras usa un teclado físico externo. Esta función resulta útil cuando usa dispositivos Android con un teclado estándar externo para PC con Windows. Similar al uso de la función DeX de Samsung.

Con Scancode, puede usar la distribución del teclado del VDA en lugar del teclado virtual de Android. De esta forma, puede adoptar completamente el estilo de entrada de Windows en lugar de usar el de Android. Eso resulta muy útil cuando se escribe en idiomas de Asia oriental, ya que mejora significativamente la experiencia general del usuario. Es posible que el usuario final use la distribución del teclado del servidor en lugar de usar la del cliente. Para obtener más información, consulte la sección Caso de uso de este artículo.

Cómo utilizar la función

Para usar la función Scancode:

1. Abra la aplicación Citrix Workspace para Android y vaya a **Ajustes > General > Teclado**.
2. Toque **Modo de entrada de teclado externo**.



3. Seleccione una de estas opciones:

- **Scancode:** Envía la posición de la tecla del teclado del lado del cliente al VDA y el VDA genera el carácter correspondiente. Aplica la distribución del teclado del lado del servidor.
- **Unicode:** Envía la tecla del teclado del lado del cliente al VDA, y el VDA genera el mismo carácter en el VDA. Aplica la distribución del teclado del lado del cliente.

De forma predeterminada, **Unicode** está seleccionado como modo de entrada del teclado externo.

4. Toque **Scancode**.

Durante una sesión, puede cambiar el teclado remoto mediante la función IME y la entrada en la distribución del teclado del servidor.

Caso de uso

Por ejemplo, imagine una situación en la que usa una distribución de teclado internacional de EE. UU. conectada a su dispositivo Android.

Si elige **Scancode** y pulsa la tecla situada junto a Bloq Mayús en el teclado externo, el código de escaneo 1E se envía al VDA. A continuación, el VDA usa 1E para mostrar el carácter **a**.

Si elige **Unicode** y pulsa la tecla situada junto a Bloq Mayús en el teclado externo, el carácter **a** se envía al VDA. Por lo tanto, aunque el VDA utilice otra distribución de teclado con un carácter diferente en la misma posición, en la pantalla se mostrará el carácter **a**.

Nota:

Unicode es el modo preferido para escribir cuando se utiliza un teclado táctil en dispositivos móviles. Esto se debe a que las teclas de un teclado táctil no suelen generar un código de escaneo.

Compatibilidad con cámaras web externas

La aplicación Citrix Workspace para Android ahora es compatible con cámaras web conectadas externamente en las sesiones. Conecte una cámara web USB y úsela para realizar videoconferencias. Para ello, toque el icono de la cámara y después seleccione el nombre de la cámara web externa. Mejora la experiencia en las sesiones al aprovechar los recursos disponibles para los usuarios finales.

Nota:

El nombre de la cámara web externa solo se muestra después de detectarse una cámara externa.



La próxima vez que use una aplicación de videoconferencia, el sistema recordará sus preferencias y utilizará la preferencia de cámara en consecuencia. Por ejemplo, si se finalizó la última videollamada con una preferencia de cámara web externa, la próxima vez se seleccionará de forma predeterminada esa cámara web externa.

Para cambiar las preferencias de la cámara, toque el icono de la cámara en la pantalla. También puede cambiar las preferencias de la cámara durante las llamadas.

Nota:

- Al quitar la cámara externa, el icono flotante de varias cámaras  cambia a un botón de voltear . El cuadro de diálogo **Seleccionar cámara** se cierra si está abierto y la vista de cámara externa del VDA deja de responder.
- Esta función es aplicable tanto en las implementaciones locales como en la nube.

Asignación de unidades del cliente

La aplicación Citrix Workspace informa al servidor de las unidades de cliente disponibles. De forma predeterminada, a las unidades del cliente se les asignan letras de unidad del servidor, de manera que parezca que están directamente conectadas a la sesión. Estas asignaciones están disponibles solamente para el usuario durante la sesión actual.

Nota:

Esta función solo es compatible con versiones de Android con SDK que tengan la versión 24 o una posterior.

La asignación de unidades de cliente (CDM) permite dispositivos de almacenamiento plug-and-play

en una sesión. Por lo tanto, puede utilizar dispositivos de almacenamiento masivo (como, por ejemplo, unidades extraíbles) para copiar y pegar documentos entre la unidad extraíble y el dispositivo del usuario.

Además, si el parámetro de CDM está configurado como acceso total o acceso de lectura, puede utilizar el almacenamiento interno del dispositivo como una unidad asignada a la sesión.

Limitaciones de la función:

- Se ha constatado que las API de Android son lentas, lo que retrasa ciertas operaciones.
- La asignación CDM para almacenamiento externo no es compatible con dispositivos Pixel.
- La asociación de tipos de archivo no se admite en dispositivos de almacenamiento externos.

Problema conocido de la función:

- La pantalla de la aplicación Workspace puede cambiar entre primer plano y segundo plano al conectar un dispositivo de almacenamiento externo.

Mejora de la asignación de unidades de cliente

Antes se aplicaba una opción seleccionada de almacenamiento del dispositivo para todos los almacenes configurados.

A partir de la versión 20.8.0, la aplicación Citrix Workspace le permite seleccionar una opción de almacenamiento del dispositivo dedicada para cada almacén configurado.

Durante el inicio de sesión, aparecerá un mensaje para seleccionar el tipo de almacenamiento del dispositivo, junto con los detalles del almacén. Puede realizar una de las siguientes acciones:

- Seleccione una de las opciones de almacenamiento del dispositivo y toque **Aceptar**: esa selección se aplicará solo a la sesión actual. En cada inicio, aparece un mensaje para que seleccione el tipo de almacenamiento del dispositivo.
- Seleccione una de las opciones de almacenamiento del dispositivo, seleccione **No volver a preguntar** y toque **Aceptar**: esa selección se aplicará a todos los inicios de sesión de ese almacén. No se le volverá a preguntar.
- Seleccione **Cancelar**: Se le pedirá que seleccione un tipo de almacenamiento del dispositivo en cada inicio y también dentro de una sesión. La sesión no tiene acceso al almacenamiento del dispositivo.

Nota:

Esta función solo se aplica en los inicios directos de ICA y en los almacenes configurados de Citrix Gateway. Es compatible con almacenes que tienen una configuración SSL de extremo a extremo.

Citrix Casting

Citrix Casting 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.

Con Citrix Casting, puede:

- Moverse por su sesión sin iniciar una sesión VDA en los dispositivos móviles.
- Para consultar la lista de Workspace Hubs disponibles, toque **Ver lista de hubs** desde el cuadro de diálogo de **Workspace Hub**.

Configuración de Citrix Casting

Citrix Casting se habilita cuando se cumplen todos estos requisitos del sistema:

- Aplicación Citrix Workspace 1809 para Android o una versión posterior
- Bluetooth habilitado
- Ubicación habilitada
- El dispositivo móvil y Workspace Hub deben utilizar la misma red Wi-Fi

Para activar la función Citrix Casting, toque **Parámetros** y **Citrix Casting** en su dispositivo.

Para obtener más información sobre Citrix Ready Workspace Hub en la aplicación Citrix Workspace, consulte [Configurar Citrix Ready Workspace Hub](#).

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

Tarjeta inteligente USB

La aplicación Citrix Workspace admite lectores de tarjetas inteligentes USB con StoreFront. Si están habilitadas, puede usar tarjetas inteligentes USB con estos fines:

- Inicio de sesión con tarjeta inteligente - Autentica usuarios a la aplicación Citrix Workspace.
- Compatibilidad con aplicaciones de tarjetas inteligente: Permite que las aplicaciones publicadas compatibles con tarjetas inteligentes puedan acceder a dispositivos de tarjetas inteligentes locales.

La aplicación Citrix Workspace admite esta función en todos los dispositivos Android incluidos en [Biometric Associates](#).

La aplicación Citrix Workspace admite los siguientes tipos de tarjetas inteligentes USB:

- Tarjetas Personal Identity Verification (PIV)
- Tarjetas CAC (Common Access Card)

Las tarjetas inteligentes USB se admiten en el sistema operativo Android desde la versión 7.x hasta la 11.x.

También puede habilitar la autenticación con tarjeta inteligente USB desde **Parámetros > Administrar cuentas**.

Configurar una tarjeta inteligente USB

Requisito previo:

- Descargue e instale el servicio Android PC/SC-Lite desde Google Play Store.
1. Conecte el lector de tarjetas inteligentes USB al dispositivo móvil. Para obtener información sobre cómo conectar lectores de tarjetas inteligentes, consulte las especificaciones del lector de tarjetas inteligentes proporcionadas por el fabricante.
 2. Agregar una cuenta de StoreFront que tenga una tarjeta inteligente habilitada
 3. En la página de inicio de sesión de la aplicación Citrix Workspace, toque **Agregar cuenta**. Toque la opción **Usar tarjeta inteligente**.
 4. Para modificar una cuenta existente para usar la autenticación con tarjeta inteligente USB, toque **Cuentas > Modificar**, y toque la opción **Usar tarjeta inteligente**.

Función para la redirección de cámaras web

Ahora puede redirigir la cámara frontal de su dispositivo a la sesión. Se admiten aplicaciones de 32 y 64 bits. De forma predeterminada, la redirección automática de la cámara web está inhabilitada.

Compatibilidad con la redirección de la cámara frontal y trasera

Ahora, la aplicación Citrix Workspace para Android le permite cambiar de la cámara frontal a la trasera y viceversa dentro de la sesión HDX. Se admiten aplicaciones de 32 y 64 bits.

Aparece un botón flotante al invocar la cámara. Toque una vez en el botón flotante para cambiar entre la cámara frontal y la trasera. También puede mover el botón flotante libremente por la pantalla y colocarlo donde quiera.

Problemas conocidos de la función

- El botón flotante queda tapado parcial o totalmente cuando la función de proyección o la función de escaneo de documentos se habilitan.

Compatibilidad con micrófono externo

Antes, la aplicación Citrix Workspace para Android solo admitía la redirección de audio a través del micrófono del dispositivo.

A partir de la versión 23.10.5, la aplicación Citrix Workspace para Android admite micrófonos externos. Los micrófonos pueden ser dispositivos periféricos USB o Bluetooth.

Tras conectar un micrófono USB o Bluetooth, el audio se redirige desde el micrófono externo a la sesión. Al retirar el micrófono externo del dispositivo, el audio se redirige automáticamente al micrófono del dispositivo.

Esta función es útil cuando se conecta un micrófono externo, por ejemplo, a un(a):

- teléfono
- tableta
- televisor inteligente
- monitor externo en una sala de conferencias.

Prolongar pantalla

March 22, 2024

Compatibilidad con Zebra Workstation Connect

Esta versión es compatible con las funciones de la tableta Zebra: iniciador de escritorio y experiencia en modo escritorio. La experiencia de usuario de la tableta Android se refleja en el monitor del cliente con Zebra Workspace Connect.

La aplicación Citrix Workspace admite estos dispositivos Zebra:

- Equipos móviles EC50, EC55, ET56
- TC52x,
- TC57x,
- TC52ax,
- TC52x-HC

- TC52ax-HC

Para obtener más información sobre la administración del dispositivo Zebra, consulte [Administrar dispositivos Zebra Android](#) en la documentación de Citrix Analytics for Performance.

Compatibilidad con varias pantallas en Samsung DeX

Samsung DeX (Desktop eXperience) está disponible en algunos dispositivos portátiles Samsung de gama alta. La función DeX le permite convertir su dispositivo en una experiencia similar a la de un escritorio mediante la conexión de un teclado, un mouse y un monitor.

Puede conectar el dispositivo compatible con DeX y la pantalla externa para prolongar la sesión de escritorio a la pantalla externa. La pantalla externa debe ser compatible con el protocolo DeX. Puede prolongar o mostrar contenido diferente en la pantalla de Samsung DeX y en la pantalla externa.

Importante:

- Esta función solo se aplica a la plataforma Samsung DeX y no a Chrome OS ni a otros dispositivos Android.
- Esta función solo es para sesiones de escritorio de Citrix y no para sesiones de aplicaciones.
- El icono **Prolongar** solo está disponible en la pantalla DeX. Inicie la sesión de escritorio desde la pantalla DeX.
- La resolución de la pantalla externa depende del dispositivo Samsung DeX, la pantalla externa y el resto del hardware utilizado.

Configurar el modo Prolongar

Para habilitar el modo **Prolongar**:

1. Conecte el dispositivo que tiene el protocolo Samsung DeX al monitor externo mediante el cable. También puede conectar el dispositivo compatible con Samsung DeX al monitor Samsung. El monitor Samsung debe ser compatible con el protocolo DeX en el modo inalámbrico.

Nota:

La configuración funciona mejor con adaptadores USB-C HDMI y USB-C Dock.

2. Abra la aplicación Citrix Workspace e inicie una sesión de escritorio desde la pantalla Samsung DeX.
3. Vaya a la barra de herramientas y toque el icono **Prolongar**.



Sugerencia:

Para quitar la extensión de pantalla, toque el icono **Prolongar** de nuevo.



4. Utilice la función para arrastrar y colocar para mover la ventana de la aplicación al monitor externo.

Limitación:

Suelte el puntero del mouse en el borde de la pantalla cuando arrastre una ventana a otra pantalla. Continúe la acción para arrastrar y colocar con un mouse desde la pantalla de destino para mover la ventana.

Nota:

- Puede girar la pantalla del dispositivo para adaptarla a sus necesidades.
- Ajuste el tamaño de la fuente para facilitar la lectura en los parámetros de visualización de la sesión de la sección **Escala y diseño**.

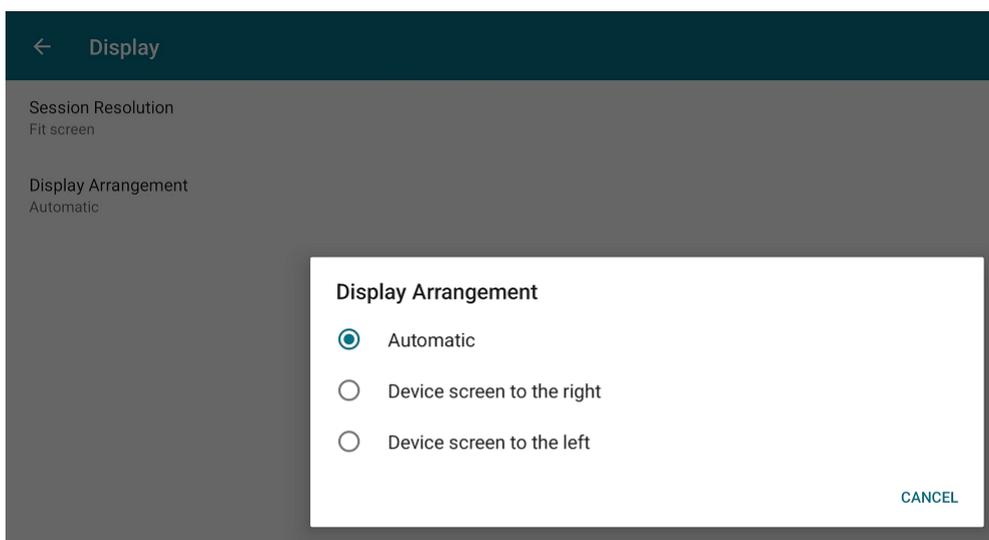
Configurar la disposición de las pantallas

Para configurar la disposición de las pantallas:

Requisito previo:

Configure la disposición de las pantallas antes de iniciar la sesión.

1. Abra la aplicación Citrix Workspace y vaya al icono de **Parámetros > Parámetros > General > Pantalla > Disposición de las pantallas**.



2. Seleccione una opción adecuada.

La pantalla del dispositivo aparece a la derecha o a la izquierda.

Importante:

- La pantalla Samsung DeX es la pantalla principal.
- Solo una pantalla puede mostrar la IU de la aplicación Citrix Workspace.
- Solo puede conectar una pantalla externa.
- La aplicación Citrix Workspace se cierra al iniciar una sesión.

Experiencia de usuario

March 22, 2024

Tiempo de espera por inactividad en sesiones de la aplicación Citrix Workspace

El administrador puede especificar el tiempo de inactividad permitido. Una vez transcurrido el tiempo de espera indicado, aparece un mensaje de autenticación.

El valor del tiempo de espera por inactividad se puede establecer desde 1 minuto hasta 24 horas. De forma predeterminada, el tiempo de espera por inactividad no está configurado. El administrador puede configurar la propiedad **inactivityTimeoutInMinutesMobile** mediante un módulo de PowerShell. Toque [aquí](#) para descargar los módulos de PowerShell de la configuración de la aplicación Citrix Workspace.

Cuando haya alcanzado el valor de tiempo de espera especificado, la experiencia del usuario final será la siguiente, según el tipo de autenticación configurado:

- Cuando se agote el tiempo de espera por inactividad, recibirá un mensaje para proporcionar una autenticación biométrica, que le permitirá acceder de nuevo a la aplicación Citrix Workspace.
- Si puede cancelar la solicitud de autenticación biométrica, aparece este mensaje:

La aplicación Citrix Workspace está bloqueada.

Debe autenticarse para seguir utilizando la aplicación Workspace.

- Si el código de acceso no está configurado en Android, debe iniciar sesión con las credenciales una vez transcurrido el tiempo de espera por inactividad.

Nota:

Esta función solo se aplica a clientes de Workspace (nube).

Función para autenticación biométrica tras inactividad

Una vez que caduca el temporizador de inactividad, se le pide al usuario final que se autentique mediante funciones biométricas como el reconocimiento facial y el escaneo de huellas digitales.

La forma más fiable de autenticación biométrica disponible para el usuario final depende del OEM de su dispositivo y se le pedirá usarla como corresponda en cada caso.

Para obtener más información sobre la configuración del temporizador de inactividad, consulte [Tiempo de espera por inactividad en sesiones de la aplicación Citrix Workspace](#).

Opción para inhabilitar la visualización de mensajes de error

Ahora puede inhabilitar la visualización del siguiente mensaje de error relacionado con la supervisión de red:

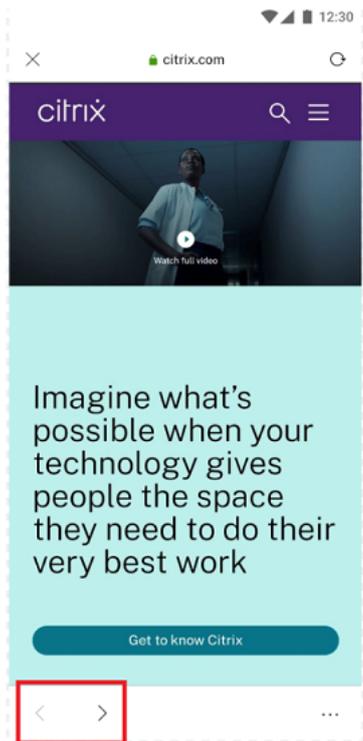
“Puede que la conexión se ralentice de forma temporal”.

Para inhabilitar el mensaje de error relacionado con problemas de red en una sesión, vaya a **Avanzado** y seleccione la opción **Inhabilitar mensajes de supervisión de red**.

Mejora de la interfaz de usuario

- A partir de la versión 20.7.0, puede quitar los detalles de la cuenta de almacén a través de la opción **Modificar**. Toque **Quitar cuenta** para quitar los detalles de la cuenta.
- A partir de la versión 20.7.5, la ficha **Recientes** muestra las aplicaciones móviles nativas junto con las aplicaciones y escritorios publicados.
- A partir de la versión 20.10.0, la aplicación Citrix Workspace admite los requisitos actuales de la API de destino de Google Play para Android 10.
- A partir de la versión 20.10.0, recibirá una notificación sobre conexiones no seguras cuando intente agregar un almacén HTTP.
- A partir de la versión 21.3.5, puede navegar hacia adelante y hacia atrás en aplicaciones web y de software como servicio (SaaS).

En su teléfono móvil, los botones de navegación aparecen en la parte inferior izquierda de la sesión de las aplicaciones SaaS y web de su espacio de trabajo.

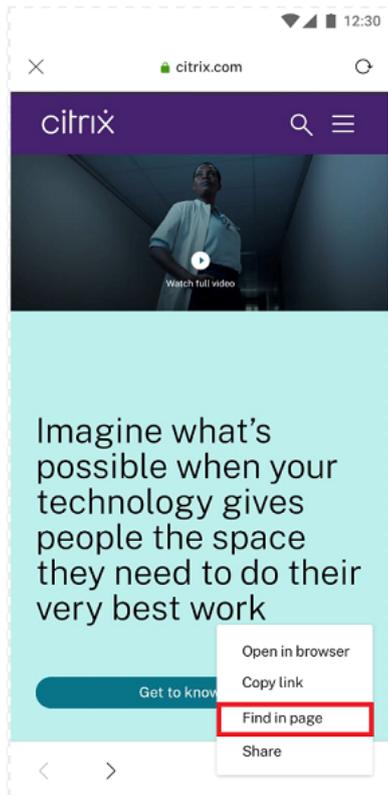


Los botones de navegación aparecen en la parte superior izquierda de la sesión de la aplicación SaaS de su tableta.

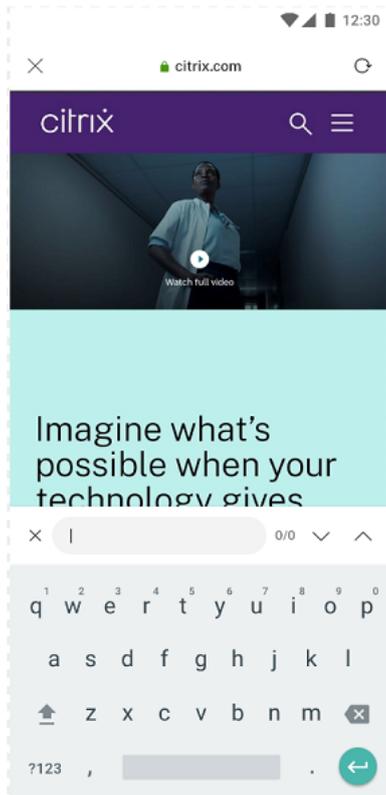
- A partir de la versión 21.4.0, puede buscar palabras o frases en sus aplicaciones web y SaaS.

Para realizar las búsquedas, siga estos pasos.

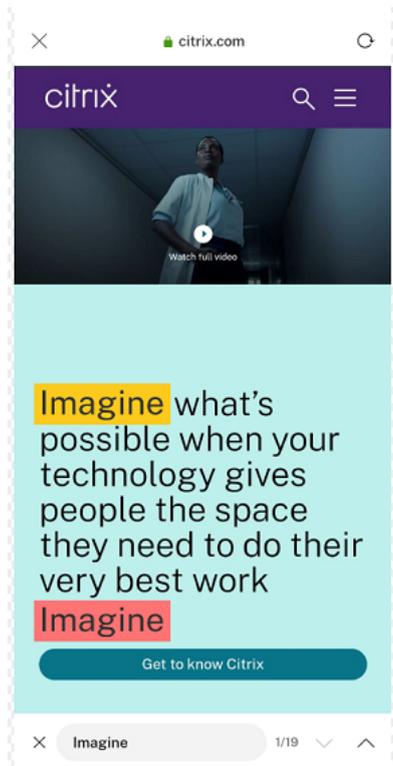
1. Toque el botón de puntos suspensivos situado en la parte inferior derecha y seleccione **Buscar en la página**.



1. Aparecerá el teclado.



1. Al escribir, aparece el resultado de la búsqueda (por ejemplo, la palabra “imagine”).



- A partir de la versión 21.6.0, puede descargar archivos de texto, audio y vídeo (con y sin enlaces directos). Para archivos de texto, audio y vídeo con enlaces directos, toque el enlace para descargarlos directamente. Puede obtener una vista previa de los archivos de audio y vídeo antes de descargarlos.

Para descargar archivos sin enlaces directos, toque el botón de puntos suspensivos de la parte inferior derecha y seleccione **Descargar**.

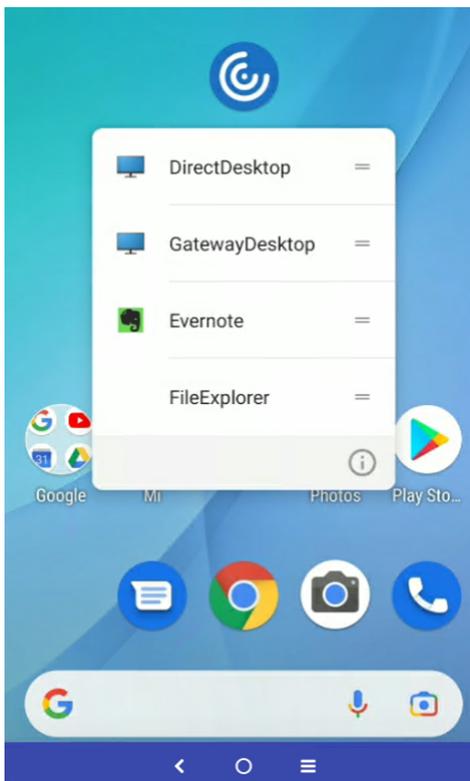
Aplicación Citrix Workspace para Android



Una vez finalizada la descarga, una notificación indica que el archivo se guardó en su carpeta de descargas.



- A partir de la versión 21.8.5, ahora admitimos la Beta 4 de Android 12 en la aplicación Citrix Workspace para Android. La actualización de la versión de la aplicación Citrix Workspace a la versión 21.8.5 garantiza un desarrollo y una asistencia ininterrumpidos para los dispositivos que se actualizan a la Beta 4 de Android 12.
- A partir de la versión 21.9.0, la aplicación Citrix Workspace admite la Beta 4 de Android 12. Si se halla en almacenes HTTP, para obtener un contexto protegido, le recomendamos pasar a almacenes HTTPS. Para obtener más información, consulte [HTTPS](#).
- A partir de la versión 22.2.0, puede acceder a una lista de aplicaciones iniciadas recientemente para un acceso rápido al tocar y mantener presionado el icono de la aplicación Citrix Workspace.



Integración del Asistente de Google

Puede interactuar con el Asistente de Google para iniciar recursos como aplicaciones y escritorios sin tener que iniciar la aplicación Citrix Workspace cada vez. Todos los recursos abiertos recientemente se enumeran en los accesos directos del Asistente de Google. Seleccione los que prefiera agregar en un acceso directo.

Para llevar a cabo la configuración:

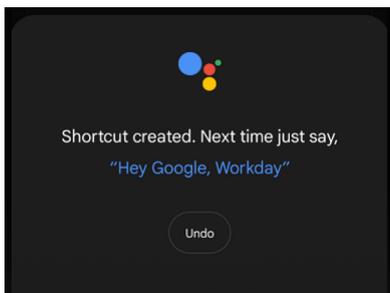
1. Inicie la aplicación Citrix Workspace y abra el recurso que quiere agregar en un acceso directo.
2. Abra los parámetros del Asistente de Google desde su dispositivo.

Nota:

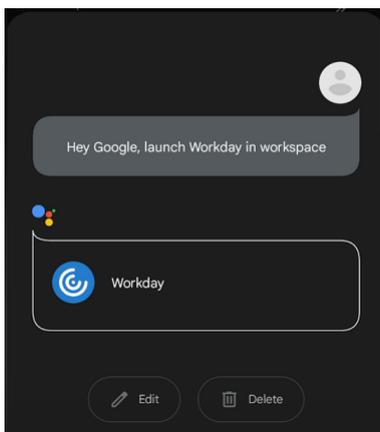
El acceso a los parámetros del Asistente de Google puede variar según la versión de Android y el dispositivo Android que utilice.

Aconsejamos usar el comando de voz para abrir los parámetros del Asistente de Google.

3. Desplácese hacia abajo y toque **Shortcuts**.
4. Toque **Citrix Workspace app** y seleccione el recurso que quiere agregar en un acceso directo. Ya puede usar comandos de voz para iniciar el recurso.



5. (Opcional) Puede modificar y actualizar el comando de voz.



Experiencia en las sesiones

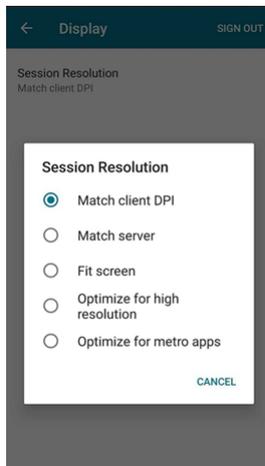
June 26, 2024

Equiparación de PPP

La función Equiparación de PPP garantiza que la sesión virtual se genere de acuerdo con los PPP del dispositivo. Anteriormente, incluso en teléfonos móviles y tabletas con valores altos de PPP, no se

tenían en cuenta los PPP del dispositivo para visualizar la sesión. A partir de la versión 24.1.0, un nuevo parámetro de la pantalla ayuda a conseguir la equiparación de PPP.

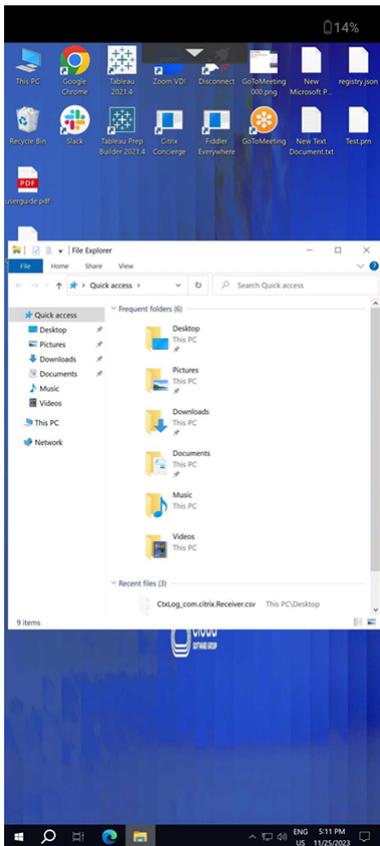
En su dispositivo, vaya a la aplicación Citrix Workspace para Android > **Parámetros** > **General** > **Pantalla** > **Resolución de la sesión** > y seleccione la opción **Equiparar PPP del cliente**.



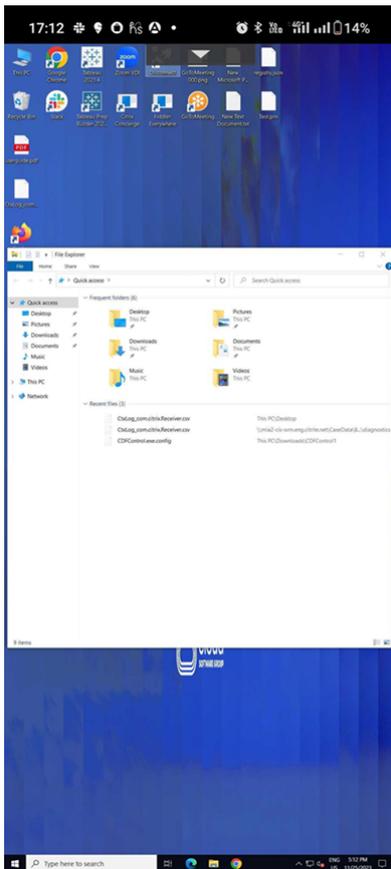
En otras palabras, la aplicación Citrix Workspace intenta equiparar automáticamente la resolución de la pantalla y los parámetros de escalado de PPP del dispositivo Android con la sesión de Citrix. Esta función mejora la experiencia del usuario al presentar las sesiones en función de los PPP disponibles del teléfono o la tableta. Ahora, los iconos, el texto y la claridad de la imagen de la sesión son más nítidos y cómodos de leer.

Por ejemplo, al seleccionar la opción **Equiparar PPP del cliente**, los iconos, el texto y las imágenes de la sesión se muestran nítidos.

Aplicación Citrix Workspace para Android



Por el contrario, al seleccionar la opción **Ajustar a la pantalla**, los iconos, el texto y las imágenes de la sesión tienen un tamaño más pequeño.



Nota:

Cuando conecta un monitor externo, la sesión continúa generándose con los PPP del dispositivo principal debido a la limitación de Android.

Enlightened Data Transport (EDT)

En versiones anteriores, había sesiones que no se iniciaban correctamente cuando no se podían establecer conexiones Enlightened Data Transport (EDT) entre Citrix Gateway y el VDA. A partir de la versión 21.5.0, las conexiones EDT fallidas recurren a TCP.

Parámetros de pila EDT habilitados de forma predeterminada

A partir de la versión 21.7.0, los parámetros de pila EDT están habilitados de forma predeterminada. Como resultado, hemos quitado la opción **Parámetros de pila EDT** de **Parámetros > Avanzado**.

Hasta ahora, la opción de inhabilitar los parámetros de pila EDT estaba disponible para los usuarios. Con esta opción disponible, no todos los clientes seguían los requisitos personalizados de tamaño de segmento máximo (MSS) de EDT de forma regular. Como resultado, la fragmentación se producía con la degradación del rendimiento de HDX y problemas al establecer sesiones para estos clientes. Con los

parámetros de pila EDT recién habilitados de forma predeterminada, la satisfacción y la experiencia general de los usuarios han mejorado.

Conexión en paralelo

A partir de la versión 21.7.0, presentamos la función de conexión paralela EDT y TCP. La función reduce los tiempos de conexión.

Antes, al establecer una conexión, la aplicación Citrix Workspace intentaba conectarse mediante EDT. Los intentos de conexiones con EDT fallidas recurrían a TCP, lo que provocaba estos problemas, que ahora se han resuelto:

- Aumento del tiempo de conexión en casos de recurrencia.
- La fiabilidad de la sesión y la reconexión automática de clientes tendían a favorecer a TCP.
- Se necesitaba detener la conexión para volver a intentar la conexión TCP.

Funciones de detección de MTU agregadas a EDT

Hemos agregado funciones de detección de unidades de transmisión máxima a Enlightened Data Transport (EDT). Como resultado, ahora puede disfrutar de una experiencia de HDX estable, proporcionada por EDT.

Antes, EDT fallaba en varios casos, como en conexiones VPN, Wi-Fi, 4G o 3G, y en Microsoft Azure, causadas por la pérdida de paquetes debido al tamaño de los paquetes.

Al intentar iniciar una sesión, la fragmentación de paquetes provocaba la desconexión de sesiones. Como solución temporal, era necesario ajustar el tamaño máximo de segmento (MSS) de EDT en el archivo de StoreFront, lo que implicaba una configuración adicional. Al agregar las *funciones de detección de MTU* a EDT, estos problemas quedan resueltos.

Las funciones de detección de MTU agregadas a EDT funcionan en sesiones alojadas en VDA 1912 y versiones posteriores.

Inicio automático del archivo ICA

Puede tocar el recurso correspondiente para iniciar sus aplicaciones y escritorios publicados. Esta función requiere la versión 1912 de StoreFront (local) o una posterior.

Inicio mejorado de sesiones

Las aplicaciones y escritorios publicados se inician en ventanas separadas. Esta mejora le ayuda a usar la ventana de enumeración de almacén e interactuar con ella sin tener que desconectar ni cerrar

la sesión.

Limitaciones:

- Después de cambiar cualquier parámetro de usuario, debe volver a iniciar la sesión para que los cambios surtan efecto.
- Las aplicaciones y el escritorio se denominan “Espacio de trabajo” en la barra de tareas; no adquieren el nombre a partir de la sesión.

Indicador de estado de la batería

Ahora el estado de la batería del dispositivo se muestra en el área de notificaciones de las sesiones de Citrix Desktop.

Nota:

El indicador de estado de la batería no se muestra para el VDA del servidor.

Redirección de dispositivos USB

A partir de la versión 20.9.0, la función de redirección de USB es totalmente funcional y está lista para la disponibilidad general. De forma predeterminada, la función de redirección de USB está inhabilitada.

Esta función permite la redirección de dispositivos USB arbitrarios desde máquinas cliente a Citrix Virtual Apps and Desktops y Citrix DaaS. Esto le permite interactuar con una amplia selección de dispositivos USB genéricos en una sesión como si estuvieran conectados físicamente a ella.

Como requisito previo para administrar esta función mediante Citrix Global App Configuration Service, debe **habilitar** la función de redirección de USB en el Delivery Controller. Para obtener más información sobre cómo configurar la redirección de USB en el Delivery Controller, consulte la sección [Dispositivos USB genéricos](#) de la documentación de Citrix Virtual Apps and Desktops.

Citrix Global App Configuration Service ofrece a los administradores de Citrix la capacidad de entregar direcciones URL de servicio de Citrix Workspace y parámetros de la aplicación Citrix Workspace a través de un servicio administrado de forma centralizada.

La función de redirección de USB está integrada y se puede configurar a través de Citrix Global App Configuration Service. Puede administrar la función mediante Citrix Global App Configuration Service en el caso de redes no conectadas a dominios.

Para obtener información sobre cómo configurar la función con este método, consulte [Global App Configuration Service](#) en la documentación para desarrolladores.

Nota:

Esta función está disponible para el público a partir de la versión 20.9.0. En la versión 20.8.1 y en las versiones anteriores, solo está disponible si se solicita.

La directiva Redirección de USB debe establecerse en **Permitida** en el Delivery Controller. Para obtener información sobre cómo configurar la redirección de USB en Citrix Studio, consulte [Configurar la redirección de USB genérico](#) en la documentación de Citrix Virtual Apps and Desktops.

Para impresoras y escáneres:

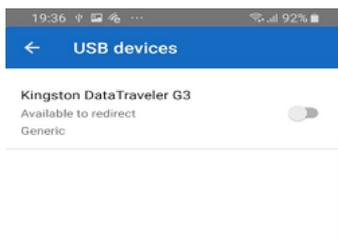
Instale los controladores específicos del proveedor en el dispositivo. Una vez finalizada la instalación, es posible que el software del proveedor pida que vuelva a conectar el dispositivo USB. Vuelva a conectar el dispositivo USB para redirigirlo.

Configurar la redirección de USB en teléfonos móviles, tabletas y Samsung DeX

1. Agregue un almacén habilitado para directivas de redirección de USB e inicie una sesión.
2. Toque el icono de la barra de herramientas de la sesión como se muestra en el siguiente cuadro de diálogo:

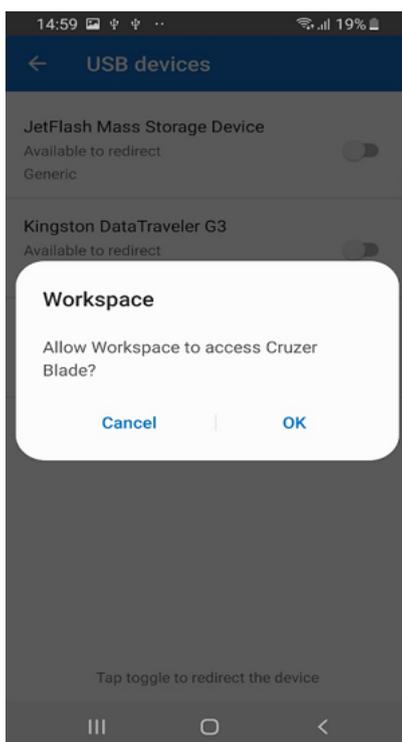


3. Toque el **icono USB** de la barra de herramientas de la sesión.
4. Los dispositivos USB conectados aparecen en la ventana de dispositivos USB como se muestra a continuación:



5. Para redirigir un dispositivo USB concreto, toque la opción Alternar situada junto al dispositivo en cuestión.

Aparecerá un cuadro de diálogo de permisos de Workspace.

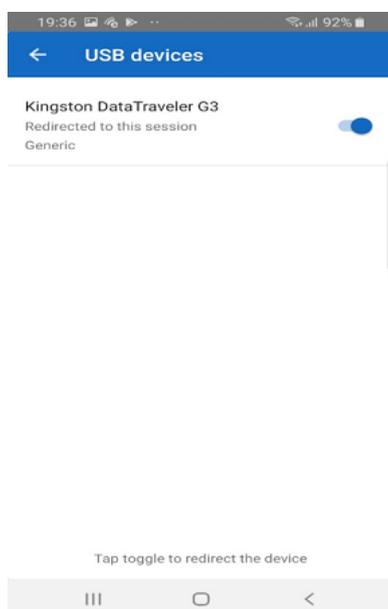


6. Toque **Aceptar** para conceder permiso para que la aplicación Citrix Workspace redirija el dispositivo.

Nota:

Este paso es obligatorio para redirigir el dispositivo USB.

El dispositivo USB se redirige y el estado se muestra de esta manera:

**Nota:**

- Si se redirige una unidad USB, aparecerá como aparece en una sesión.
- Si se redirige una impresora o un escáner, se muestra en la sección **Dispositivos** del panel de control.

Dispositivos USB probados

Dispositivo	Fabricante	Modelo
Impresora	HP	LaserJet P2014
Escáner	HP	Scanjet G3010
Escáner	Canon	CanoScan LiDE 700 F
SpaceNavigator	3Dconnexion	
Impresora	Brother	QL-580N
Escáner	HP	Scanjet 200

Problemas conocidos:

- No se admite más de un dispositivo USB a la vez.

- Por ahora, los dispositivos USB de audio y vídeo no son compatibles.

Redirección automática de dispositivos USB

La aplicación Citrix Workspace le permite redirigir dispositivos USB automáticamente al conectarlos. Al conectar un dispositivo USB, aparece un mensaje en el que se le pide permiso. Después de conceder el permiso, el dispositivo USB se redirige automáticamente.

Nota:

Esta función solo está disponible a demanda y solamente si la función de redirección de dispositivos USB está habilitada.

Mejoras en la redirección de audio

Antes, la redirección de audio de las sesiones de escritorio requería varios niveles de configuración del micrófono, y los pasos para establecer los permisos no eran intuitivos. Ahora, se han simplificado los parámetros de los permisos de micrófono para que sean más fáciles de usar. También puede habilitar los permisos mientras está en una sesión.

De forma predeterminada, la opción de audio en **Aplicación Citrix Workspace > Parámetros > Audio** está habilitada. Ahora, la sesión puede detectar el ponente que ya esté conectado. Los administradores pueden habilitar o inhabilitar la redirección de audio mediante [Global App Configuration Service](#).

Nota:

De forma predeterminada, el permiso de micrófono está inhabilitado tanto en el parámetro de la aplicación Citrix Workspace como en la página de configuración del almacén.

Es posible que se encuentre con uno de estos casos en los que la aplicación Citrix Workspace o el almacén inhabiliten el micrófono:

- Cuando los parámetros de la aplicación Citrix Workspace y del almacén inhabilitan el permiso del micrófono, aparece el mensaje emergente **Allow Workspace to record audio** al iniciar la sesión de escritorio y utilizar el micrófono. Toque **While using the app**.
- Cuando la aplicación Citrix Workspace habilita el permiso del micrófono, pero los parámetros del almacén lo inhabilitan, aparece el mensaje emergente **Permitir acceso al micrófono** al iniciar la sesión de escritorio y utilizar el micrófono. Toque en **Permitir**.

Sincronización de la distribución de teclado

La aplicación Citrix Workspace le permite habilitar la sincronización de la distribución del teclado en **Parámetros > General > Teclado > Sincronización de la distribución del teclado**.

La opción **Sincronizar distribución del teclado** permite sincronizar automáticamente la distribución del teclado con el agente VDA y el dispositivo del cliente.

En una instalación nueva y de forma predeterminada, el IME del lado del cliente se habilita automáticamente para japonés, chino y coreano, y la opción **Sincronización de la distribución del teclado** está **desactivada**.

Para habilitar la sincronización dinámica de la distribución del teclado, **active** la opción **Sincronización de la distribución del teclado**.

Cuando la opción de **sincronización de la distribución del teclado** está inhabilitada, tanto el IME del lado del VDA (remoto) como el IME del lado del cliente se aplicarán en función del método de entrada actual del dispositivo. Por ejemplo, si el IME del lado del cliente está en inglés y el IME del lado del VDA está en japonés, se aplica el IME del lado del VDA (remoto).

Cuando la opción de **sincronización de la distribución del teclado** está habilitada, el IME del lado del cliente tiene prioridad. Si cambia el idioma de entrada en el IME del lado del cliente, el IME del lado del VDA también cambia. Por ejemplo, si cambia el IME del lado del cliente a japonés, el IME del VDA cambia automáticamente a japonés. Al mismo tiempo, se utiliza el IME de japonés en el dispositivo cliente durante la sesión.

Requisitos previos:

- Para Linux VDA, habilite las directivas de **sincronización de la distribución del teclado del cliente y Mejora de IME**.
- Para Windows VDA, habilite las directivas **Asignación de distribución de teclado Unicode, Sincronización de la distribución del teclado del cliente y Mejora de IME**.
- La versión del VDA debe 7.16 o posterior.

Limitaciones de la función:

- Esta función solo funciona en los teclados virtuales de los dispositivos, no en teclados externos.
- La sincronización de la distribución del teclado no es compatible con Gboard (el teclado de Google).
- La distribución del teclado solo puede sincronizarse desde el cliente hacia el servidor. Cuando se cambia la distribución del teclado en el lado del servidor, la del cliente no puede cambiarse.
- Cuando se cambia la distribución de teclado del cliente a una distribución que no es compatible, es posible que se sincronice la distribución en el VDA, pero no se puede confirmar la funcionalidad.

Distribución del teclado compatible con Windows VDA y Linux VDA

Distribución del teclado en Android	Idioma del teclado	Distribución del teclado en Windows	Distribución de teclado en Linux
Bielorruso (Bielorrusia)	Bielorruso (Bielorrusia)	Teclado bielorruso (Bielorrusia)	by
Búlgaro	Búlgaro	Teclado búlgaro (máquina de escribir)	bg
Chino simplificado	Chino (simplificado, China)	IME de Citrix: chino (simplificado, China)	zh
Chino tradicional	Chino (tradicional, Taiwán)	IME de Citrix: chino (tradicional, Taiwán)	tw
Croata	Croata (Croacia)	Teclado croata	hr
Checo	Checo	Teclado checo	cz
Danés	Danés	Teclado danés	df
Neerlandés	Neerlandés (Países Bajos)	Teclado estadounidense internacional	us
Neerlandés (Bélgica)	Neerlandés	Teclado belga (punto)	be
Inglés (Australia)	Inglés (Australia)	Teclado estadounidense	us
Inglés (Canadá)	Inglés (Canadá)	Teclado estadounidense	us
Inglés (Reino Unido)	Inglés (Reino Unido)	Teclado del Reino Unido	gb
Inglés (EE. UU.)	Inglés (Estados Unidos)	Teclado estadounidense	us
Estonio	Estonio	Teclado estonio	ee
Finlandés	Finlandés	Teclado finés	fi
Francés (Canadá)	Francés (Canadá)	Teclado francés	fr
Francés (Suiza)	Francés (Francia)	Teclado francés suizo	ch
Francés (francés)	Francés (Francia)	Teclado francés	fr
Alemán (Austria)	Alemán (Austria)	Teclado alemán	at
Alemán (Suiza)	Alemán (Suiza)	Teclado alemán suizo	ch
Alemán (Alemania)	Alemán (Alemania)	Teclado alemán	at

Distribución del teclado en Android	Idioma del teclado	Distribución del teclado en Windows	Distribución de teclado en Linux
Griego	Griego	Teclado griego	gr
Húngaro	Húngaro	Teclado húngaro	hu
Islandés	Islandés	Teclado islandés	is
Irlandés	Irlandés		ie
Italiano	Italiano (Italia)	Teclado italiano	it
Japonés	Japonés	IME de Citrix: japonés	jp
Coreano	Coreano	IME de Citrix: coreano	kr
Letón	Letón	Teclado letón	lv
Noruego	Noruego (Bokmål)	Teclado noruego	no
Polaco	Polaco	Teclado polaco (programadores)	pl
Portugués (Brasil)	Portugués (Brasil)	Teclado portugués (ABNT de Brasil)	br
Portugués (Portugal)	Portugués (Portugal)	Teclado portugués	pt
Rumano	Rumano (Rumanía)	Teclado rumano (antiguo)	ro
Ruso (Rusia)	Ruso	Teclado ruso	ru
Eslovaco	Eslovaco	Teclado eslovaco	sk
Esloveno	Esloveno	Teclado esloveno	si
Español (México)	Español (México)	Teclado latinoamericano	latam
Español (España)	Español (España)	Teclado español	es
Sueco (Suecia)	Sueco (Suecia)	Teclado sueco	se
Turco	Turco	Teclado F turco	tr
Ucraniano	Ucraniano	Teclado ucraniano	ua

Continuidad del servicio

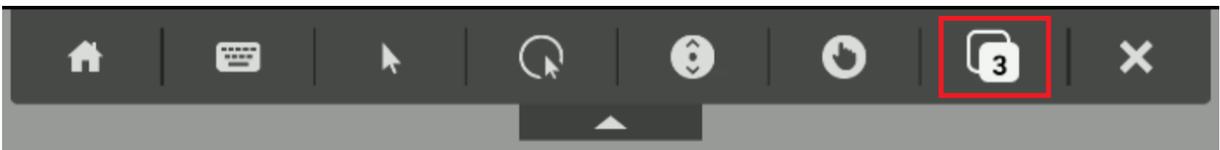
La continuidad del servicio elimina o minimiza la dependencia de la disponibilidad de los componentes involucrados en el proceso de conexión. Los usuarios pueden iniciar sus aplicaciones y escritorios virtuales, independientemente del estado de los servicios en la nube.

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

Cambio de aplicaciones

Esta función permite al usuario final cambiar entre muchas aplicaciones publicadas que están en la misma sesión. Al tocar el icono **Cambiar**, puede desplazarse hacia arriba o hacia abajo para seleccionar una aplicación, y se resalta la aplicación en el foco. Puede ver el título de la aplicación, una imagen de vista previa y el título de la ventana.

Al abrir o cerrar una aplicación, el recuento de aplicaciones se actualiza en consecuencia. Si algunas aplicaciones se abren en otra sesión, el recuento de aplicaciones incluye todas las que están abiertas.

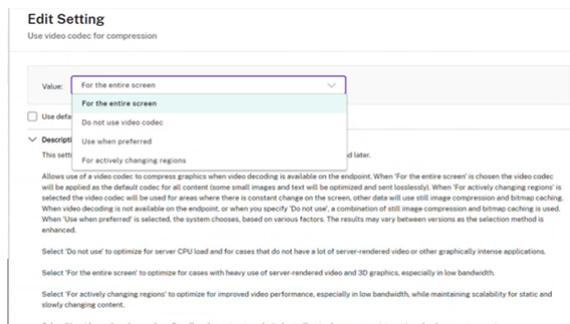


Compatibilidad con visualización a pantalla completa

A partir de la versión 23.8.0, el códec H264 admite una reproducción de vídeo mejorada en el modo de pantalla completa. Si suele ver vídeos o depende mucho de contenido de vídeo, le recomendamos esta función. Está diseñada para mejorar la visualización de vídeos en cuanto al rendimiento, la calidad del vídeo y la utilización de los recursos.

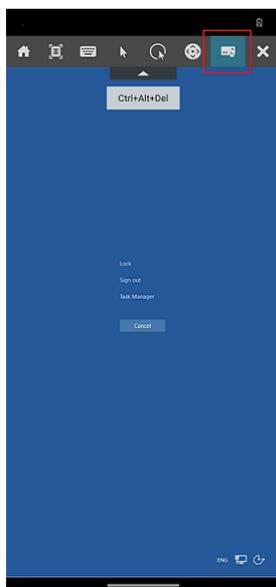
Configuración

En la máquina de DDC, defina la directiva **Usar códec de vídeo para la compresión** en **Para toda la pantalla** para mejorar la compresión de vídeo hasta 60 FPS.



Incorporación del acceso directo Ctrl+Alt+Supr a la barra de herramientas de la sesión

A partir de la versión 23.9.5, la barra de herramientas de la sesión tiene una opción para ejecutar la función Ctrl+Alt+Supr con solo tocar un botón. Esta opción facilita a los usuarios cerrar sesión, cambiar de usuario, bloquear el dispositivo o acceder al Administrador de tareas.



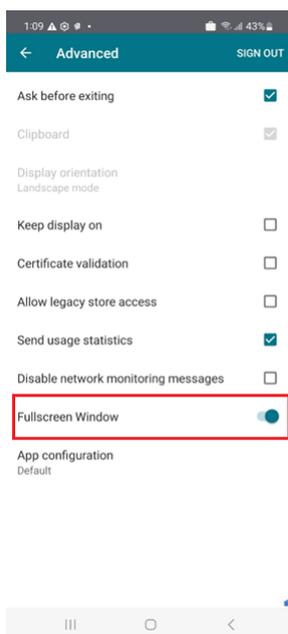
Compatibilidad con el modo de pantalla completa para sesiones de aplicación

Anteriormente, al iniciar una sesión de aplicación, se podía ver en el modo de ventana.

A partir de la versión 23.9.5, la aplicación Citrix Workspace para Android presenta una nueva opción para ver la sesión de la aplicación en modo de pantalla completa. Esta función es útil al:

- iniciar una sesión en modo de inmersión total con dispositivos táctiles
- intentar duplicar la pantalla y transmitirla
- ver la aplicación Citrix Workspace en una pantalla más pequeña.

Para habilitar la opción, en la aplicación Citrix Workspace para Android, vaya a **Parámetros > Avanzados > Ventana en pantalla completa** y actívela. En la siguiente captura de pantalla se muestra la opción:



Accesibilidad y TalkBack

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

Para usar la función TalkBack de Android, los usuarios finales deben habilitarla desde **Ajustes** de Android > **Accesibilidad** > **TalkBack**.

Para obtener más información, consulte [Accesibilidad y TalkBack](#) en la documentación de ayuda.

Problemas conocidos de la función

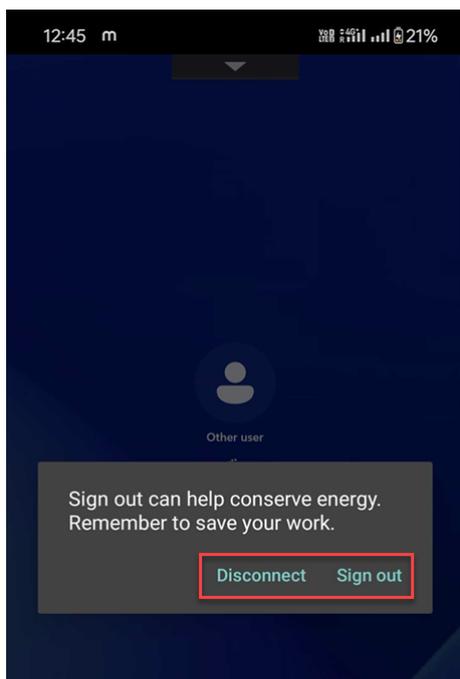
- Al conectar un teclado externo al dispositivo:
 - Al intentar usar la tecla Bloq Mayús como tecla del Narrador, es posible que la acción no funcione según lo previsto. Como solución temporal, presione la tecla Insert. [HDX-55347]
 - Al intentar usar la combinación de teclas Win+Ctrl+Intro para habilitar el Narrador, la acción no surtirá efecto dentro de la sesión de escritorio virtual. Como solución temporal, use la tecla Win o el menú Inicio e introduzca la palabra Narrador. [HDX-55380]

Iniciativa de sostenibilidad de la aplicación Citrix Workspace

Anteriormente, los escritorios virtuales permanecían en estado desconectado cuando los usuarios los cerraban tocando el botón de inicio. Eso consumía energía y recursos energéticos innecesarios.

A partir de la versión 24.2.0, hemos introducido una iniciativa de sostenibilidad que anima a los usuarios a ahorrar la energía que se podría desperdiciar al ejecutar escritorios virtuales no utilizados.

Con esta función habilitada, cuando los usuarios tocan el icono **X** para desconectar la sesión, se muestra un mensaje para cerrar sesión en la sesión de escritorio. Esta función puede resultar útil en las empresas que usan directivas del sistema operativo Windows para apagar las máquinas virtuales cuando no hay usuarios con sesiones iniciadas.



Los usuarios finales pueden salir de la sesión de dos maneras:

- **Cierre sesión** para ahorrar energía. Esta acción de sostenibilidad apaga la máquina virtual y ahorra energía. Los usuarios finales deben asegurarse de guardar su trabajo antes de cerrar sesión.
- **Desconectar** para cerrar la ventana de sesión del escritorio virtual. No obstante, la sesión virtual permanece activa hasta el siguiente inicio de sesión. Los usuarios finales pueden reanudar su trabajo fácilmente.

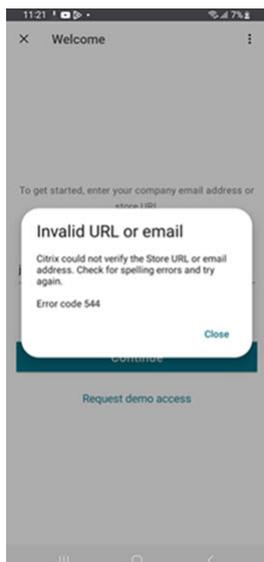
Como administrador, puede personalizar el mensaje de sostenibilidad. Para obtener más información sobre cómo habilitar y personalizar esta función, consulte el artículo [Iniciativa de sostenibilidad de la aplicación Citrix Workspace](#) en la documentación de la aplicación Citrix Workspace para Windows.

Mensajes de error mejorados

Anteriormente, los mensajes de error no contenían suficiente información útil.

A partir de la versión 23.12.0, siempre que es posible los mensajes de error incluyen un título explicativo claro, una descripción específica del error en cuestión y códigos de error. Los códigos de error sirven de ayuda a los administradores para solucionar el problema. Los mensajes mejorados dirigidos a los usuarios finales proporcionan detalles suficientes para solucionar los problemas. Si hay algún problema sin resolver, sugerimos a los usuarios que se pongan en contacto con su administrador de TI para obtener más ayuda.

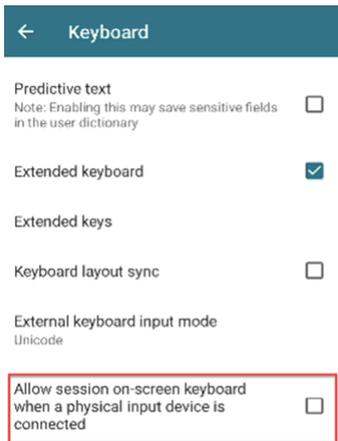
Por ejemplo, cuando el usuario no puede iniciar sesión, aparece el siguiente mensaje de error:



Compatibilidad con teclado virtual para escáner de códigos de barras

Anteriormente, cuando en una sesión se detectaban escáneres de códigos de barras (por ejemplo, los escáneres de Zebra), no se mostraba el teclado virtual. El problema era que se identificaba como un teclado externo.

A partir de la versión 24.2.0, el teclado virtual se muestra cuando los escáneres de códigos de barras están conectados como un dispositivo de entrada física. Se ha agregado un nuevo parámetro de teclado para esta función. Los usuarios finales pueden ir a **Parámetros > Teclado** en la aplicación Citrix Workspace y seleccionar la opción **Permitir sesión con teclado en pantalla cuando se conecta un dispositivo de entrada físico**.



Administrar el texto predictivo

El texto predictivo facilita la escritura al sugerir palabras que puede escribir a continuación. Al habilitar esta función durante una sesión de escritorio o de aplicación, es posible que las contraseñas aparezcan en la cinta de predicciones. Para controlar este comportamiento, esta función está inhabilitada de forma predeterminada.

Notas:

- En los parámetros de teclado predeterminados del dispositivo, si la opción **Texto predictivo** está inhabilitada, no podrá usar esta función aunque la habilite a través de la aplicación Citrix Workspace para Android.
- En una sesión, cuando se establece como predeterminada la distribución de entrada CJK en el teclado GBoard, aparece el diseño en inglés en lugar de la distribución CJK. Para ver la distribución de teclado CJK, vaya a **Parámetros > Teclado** en la aplicación y habilite la opción **Texto predictivo**. [CVADHELP-23667]

Escáner de documentos

Si ha iniciado sesión en la aplicación Citrix Workspace, puede utilizar la función de escaneo de documentos para escanear muchos documentos y transferirlos a la sesión de escritorio virtual.

Nota:

- Esta función está habilitada de manera predeterminada.

Requisitos previos

- [La asignación de unidades del cliente \(CDM\)](#) debe estar habilitada para el almacén.
- El escáner de documentos requiere acceso de lectura y escritura en el dispositivo. Para habilitar el acceso, siga estos pasos:
 1. Desde su perfil, toque **Parámetros de aplicación** > **Parámetros de almacén**.
 2. Toque su almacén actual.
 3. Toque **Almacenamiento del dispositivo** y, a continuación, seleccione **Acceso total**.

Para obtener más información sobre cómo usar esta función, consulte [Escáner de documentos](#) en la documentación de ayuda.

Experiencia en los almacenes

February 21, 2024

Usuarios no autenticados

La aplicación Citrix Workspace admite usuarios no autenticados (anónimos). Usuarios anónimos pueden iniciar correctamente sesiones de Citrix Virtual Apps and Desktops y Citrix DaaS (antes denominado Citrix Virtual Apps and Desktops Service).

Parámetros de seguridad

Citrix recomienda utilizar almacenes seguros. Además, es recomendable tener habilitado el parámetro de seguridad de transporte estricta de HTTP (HSTS) para almacenes seguros.

Siga estos pasos para habilitar el parámetro **HSTS**:

1. En **Citrix StoreFront**, en **Almacenes**, toque el enlace del almacén en particular para habilitar los parámetros de seguridad.
2. Aparecerá el cuadro de diálogo **Administrar sitios de Receiver para Web**.
3. Toque **Configurar**.
4. Aparecerá el cuadro de diálogo **Modificar sitio de Receiver para Web**.
5. Toque la ficha **Parámetros avanzados** y seleccione **Habilitar seguridad de transporte estricta**.

Autenticación

June 26, 2024

Tarjetas inteligentes

La aplicación Citrix Workspace para Android admite la autenticación mediante Citrix Gateway con los métodos siguientes, según la edición disponible:

- Sin autenticación (versiones Standard y Enterprise solamente)
- Autenticación de dominio
- Autenticación mediante envío de código de acceso por SMS (PIN de un solo uso)
- Autenticación con tarjeta inteligente

Ahora la aplicación Citrix Workspace para Android admite los siguientes productos y configuraciones.

Lectores de tarjetas inteligentes:

- BaiMobile 3000MP USB Smart Card Reader

Tarjetas inteligentes:

- Tarjetas PIV
- Tarjetas CAC (Common Access Card)

Configuraciones:

- Autenticación con tarjeta inteligente en Citrix Gateway con StoreFront 2 o 3 y Citrix Virtual Apps and Desktops 7.x y versiones posteriores.

Nota:

- Se pueden configurar otras soluciones de autenticación por token mediante RADIUS. Para la autenticación con tokens de SafeWord, consulte [Configuración de Autenticación de SafeWord](#).

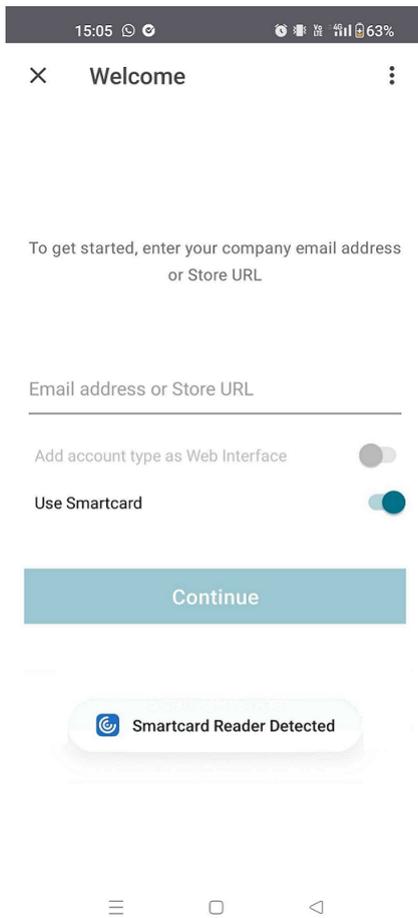
Cómo usar tarjetas inteligentes

Requisito previo

- Para usar tarjetas inteligentes, instale la [aplicación C4E desde Play Store](#). Dirección de correo electrónico de contacto: android@citrix.com para licencias.

Para usar tarjetas inteligentes para acceder a las aplicaciones:

1. Si quiere configurar la aplicación Citrix Workspace automáticamente para acceder a aplicaciones al crear una cuenta, introduzca la URL de su almacén en el campo **Dirección**. Por ejemplo:
 - .organization.com
 - netscalervserver.empresa.com
2. Inserte la tarjeta inteligente junto con el lector compatible en su dispositivo Android. La aplicación Citrix Workspace detecta automáticamente la tarjeta inteligente.



3. Seleccione la opción **Usar tarjeta inteligente** para autenticarse.

Nota:

- El acceso al almacén será válido durante aproximadamente una hora. Transcurrido ese tiempo, deberá iniciar sesión para actualizar el acceso o iniciar otras aplicaciones.

Compatibilidad con la autenticación basada en FIDO2 al conectarse a una sesión HDX

Ahora, a partir de la versión 23.8.0, la aplicación Citrix Workspace para Android admite la autenticación sin contraseña dentro de una sesión de Citrix Virtual Apps and Desktops mediante métodos de autenticación basados en FIDO2.

Esta función permite a los usuarios iniciar sesión en sitios web compatibles con WebAuthn en exploradores web. Por ejemplo, Google Chrome o Microsoft Edge utilizan autenticadores de plataforma compatibles con FIDO2, como las huellas digitales o el PIN de dispositivo. El simple hecho de abrir un sitio web compatible con WebAuthn desencadena la autenticación sin contraseña.

En FIDO2 no se admite el inicio de sesión en la aplicación Citrix Workspace o en la sesión de escritorio mediante autenticación sin contraseña.

Nota:

Los autenticadores móviles, como YubiKey o tarjetas inteligentes, no son compatibles con la aplicación Citrix Workspace para Android.

Para obtener más información sobre los requisitos previos de esta función, consulte [Autorización local y autenticación virtual mediante FIDO2](#) en la documentación de Citrix Virtual Apps and Desktops.

Tiempo de espera por inactividad en sesiones de la aplicación Citrix Workspace

El administrador puede especificar el tiempo de inactividad permitido. Una vez transcurrido el tiempo de espera indicado, aparece un mensaje de autenticación.

Para obtener más información, consulte [Tiempo de espera por inactividad en sesiones de la aplicación Citrix Workspace](#).

Función para autenticación biométrica tras inactividad

Una vez que caduca el temporizador de inactividad, se le pide al usuario final que se autentique mediante funciones biométricas como el reconocimiento facial y el escaneo de huellas digitales.

La forma más fiable de autenticación biométrica disponible para el usuario final depende del OEM de su dispositivo y se le pedirá usarla como corresponda en cada caso.

Función de autenticación mediante FIDO2 al conectarse a almacenes de la nube

A partir de la versión 24.5.0, los usuarios pueden autenticarse en la aplicación Citrix Workspace mediante la autenticación sin contraseña basada en FIDO2 al conectarse a almacenes de la nube. FIDO2 ofrece un método de autenticación integrado que permite a los empleados de la empresa acceder

a aplicaciones y escritorios dentro de sesiones virtuales sin necesidad de introducir un nombre de usuario o una contraseña. Esta función admite tanto itinerancia (solo USB) como autenticadores de plataforma (código PIN, reconocimiento facial y huella digital únicamente). Esta función es compatible con la versión 9 y posteriores de Android.

La autenticación FIDO2 es compatible con las fichas personalizadas de Chrome. Si está interesado en utilizar la autenticación FIDO2 con WebView, registre su interés utilizando el [formulario de Podio](#).

Nota:

Esta función está habilitada de manera predeterminada.

Protección

December 7, 2023

ProGuard habilitado para la seguridad

Hemos habilitado ProGuard para proteger Citrix Workspace para Android mediante la ofuscación. ProGuard cambia el nombre de diferentes partes del código para evitar la inspección de seguimientos de pila y protege la aplicación Workspace. ProGuard también reduce el tamaño de la aplicación al acortar los nombres de las clases, los métodos y los campos de las aplicaciones.

Criptografía

Esta función es un cambio importante en el protocolo de comunicación segura. Los conjuntos de cifrado con el prefijo `TLS_RSA_` no ofrecen confidencialidad directa y no se consideran robustos.

Se han quitado los conjuntos de cifrado `TLS_RSA_`. A partir de la versión 20.6.5, se admiten conjuntos de cifrado `TLS_ECDHE_RSA_` avanzados. Si su entorno no está configurado con los conjuntos de cifrado `TLS_ECDHE_RSA_`, no puede iniciar el cliente porque los cifrados no son robustos.

Se admiten los siguientes conjuntos de cifrado avanzado:

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

TLS 1.0 admite los siguientes conjuntos de cifrado:

- `TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA`

TLS 1.2 admite los siguientes conjuntos de cifrado:

- TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384
- TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384
- TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA

TLS 1.3 admite los siguientes conjuntos de cifrado:

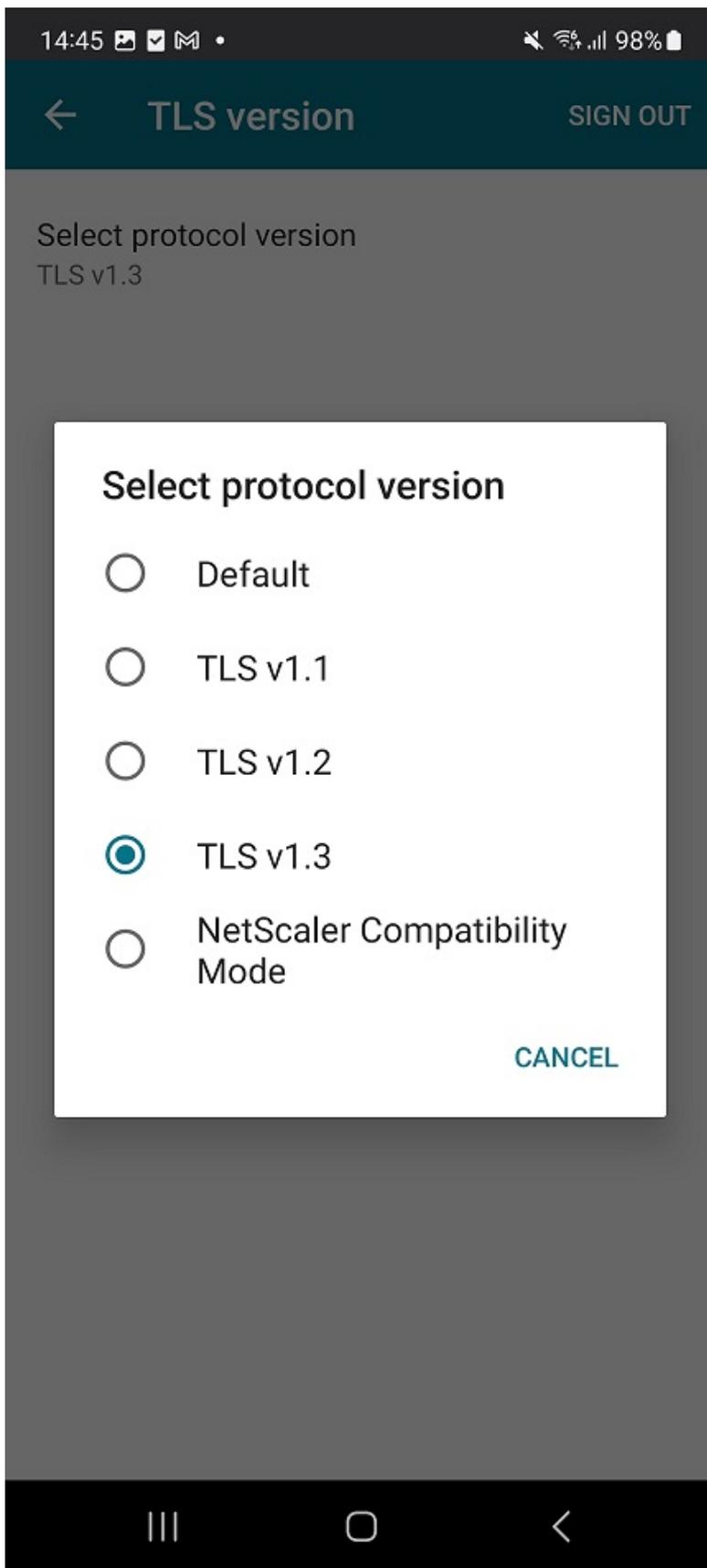
- TLS_AES_256_GCM_SHA384
- TLS_AES_128_GCM_SHA256

Compatibilidad con Transport Layer Security 1.3

Ahora, la aplicación Citrix Workspace para Android es compatible con Transport Layer Security (TLS) 1.3. Aumenta el rendimiento y la eficiencia. TLS 1.3 proporciona una gran seguridad con sus robustos conjuntos de cifrado y sus claves de sesión de un solo uso.

Los usuarios finales pueden habilitarlo en la aplicación Citrix Workspace para Android de esta manera:

1. Vaya a **Parámetros** de la aplicación Citrix Workspace > **Versión de TLS**.
2. Toque la opción **Seleccione la versión del protocolo** y seleccione **TLS v1.3**.



Para obtener más información, consulte [Criptografía](#).

Para obtener más información sobre la documentación de ayuda, consulte la [versión de TLS](#).

Solucionar problemas técnicos

March 22, 2024

Cómo comprobar la versión de la aplicación

Para saber qué versión de la aplicación Citrix Workspace está usando, consulte el artículo [Cómo comprobar la versión de la aplicación](#) en la documentación de ayuda.

Cómo actualizar a la versión más reciente

Para actualizar manualmente la aplicación Citrix Workspace a la versión más reciente, haga lo siguiente:

1. Abra Play Store.
2. Busque Citrix Workspace.

Si hay una actualización disponible, toque **Actualizar**.

Actualice la aplicación automáticamente

De forma predeterminada, las aplicaciones se actualizan automáticamente cuando se cumplen las siguientes condiciones:

- El dispositivo está conectado a una red Wi-Fi.
- El dispositivo se está cargando.
- El dispositivo está inactivo (no se usa activamente).
- La aplicación Citrix Workspace no se ejecuta en primer plano.

Nota:

Google Play Store comprueba si hay actualizaciones de las aplicaciones una vez al día. Por lo tanto, pueden pasar hasta 24 horas antes de que una actualización de la aplicación se agregue a la cola de actualizaciones. Una vez que se agregue una aplicación a la cola, se actualizará automáticamente la próxima vez que se cumplan las condiciones.

Cómo restablecer la aplicación Citrix Workspace

Para restablecer la aplicación, puede realizar una de las siguientes acciones:

- Borre los datos de almacenamiento de la aplicación Citrix Workspace. Vaya a **Ajustes** del dispositivo Android > **Aplicaciones**, seleccione la **Aplicación Citrix Workspace** > **Almacenamiento** > **Borrar caché**.
o bien
- Desinstale la aplicación Citrix Workspace e instale desde [Google Play](#) la aplicación Citrix Workspace para Android más reciente que tenga las correcciones más actualizadas.

Nota

Al eliminar las cuentas existentes de la aplicación Citrix Workspace, se restablece la cuenta y no la propia aplicación Citrix Workspace.

Cómo recopilar registros

La recopilación de registros es importante, ya que puede ayudar a identificar problemas. Para obtener más información, consulte el artículo [Cómo recopilar registros](#) en la documentación de ayuda.

Cómo enviar comentarios

Puede enviarnos sus comentarios sobre la aplicación Citrix Workspace para Android y notificar problemas desde la misma interfaz. Para obtener más información, consulte el artículo [Cómo enviar comentarios](#) en la documentación de ayuda.

Cómo solicitar mejoras

Para solicitar mejoras de las funciones de la aplicación Citrix Workspace para Android, rellene el [formulario de Podio](#).

Cómo acceder a las funciones en Technical Preview

Para conocer las funciones que se encuentran en Technical Preview, consulte [Funciones en Technical Preview](#).

Cómo enviar comentarios sobre EAR

Para enviar comentarios sobre la versión de EAR, toque [aquí](#).

Problemas comunes y consejos para solucionar problemas

Aplicación no disponible en el almacén de aplicaciones

Si no puede usar Google Play Store para instalar la aplicación Citrix Workspace para Android, como alternativa puede descargar la aplicación desde la página [Descargas de Citrix](#).

Fallos de la instalación

Si la aplicación Citrix Workspace no es compatible de forma predeterminada en Android TV, contacte con nosotros a través de [solicitudes de mejora](#).

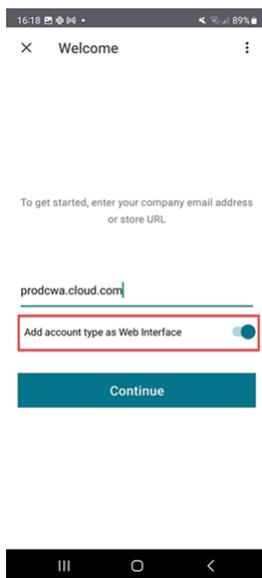
Autenticación y adición de almacenes

Si tiene problemas relacionados con la autenticación o la incorporación de almacenes, compruebe lo siguiente.

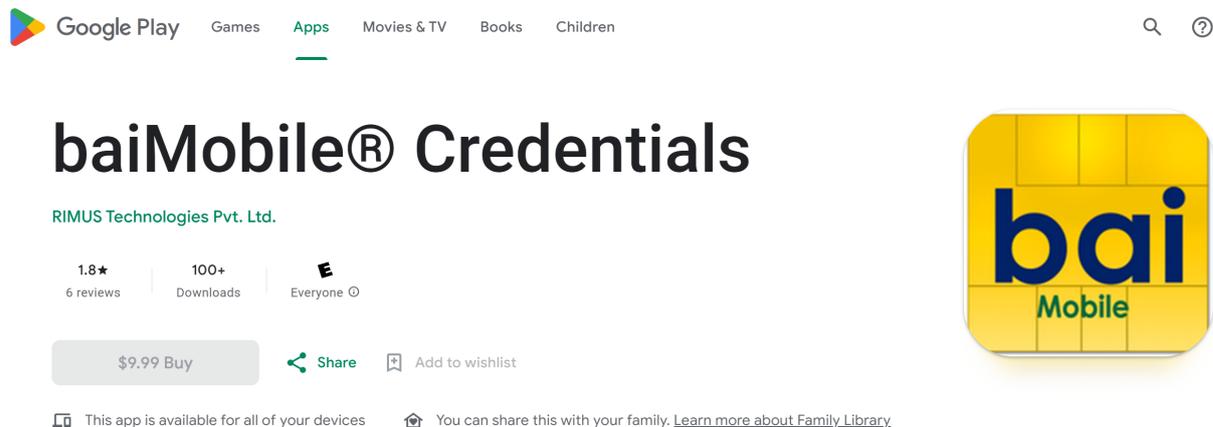
Entrada no válida Puede que haya introducido:

- credenciales no válidas
- una URL de almacén incorrecta
- errores tipográficos al introducir las credenciales y la URL del almacén
- HTTP en lugar de HTTPS.

Modo de interfaz web También puede probar a usar el modo de **Interfaz Web**. En la primera página de la aplicación, toque **Comenzar**. En la página **Bienvenida**, introduzca la URL del almacén y habilite **Agregar tipo de cuenta como Interfaz Web**.



Tarjeta inteligente Si la autenticación con tarjeta inteligente no funciona, instale la aplicación **baiMobile Credentials**. Si la aplicación baiMobile Credentials detecta su tarjeta inteligente, contacte con nosotros para investigar más a fondo el problema.



Configuraciones de directivas de NetScaler Para solucionar problemas de conexión, consulte el artículo de Knowledge Center sobre [NetScaler Gateway para dispositivos móviles](#).

Inicio de sesiones

Para ver las estadísticas de la sesión:

- desde la barra de herramientas de la sesión, toque cuatro veces el icono del puntero del mouse o bien

- ejecute el comando `ctxsession -v` en el terminal de la sesión.

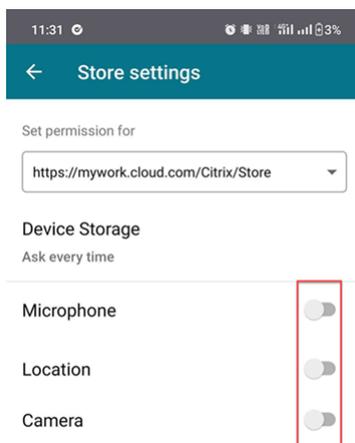
Error al iniciar el escritorio Para solucionar problemas, consulte los siguientes artículos de Knowledge Center:

- [Código de error 2524](#)
- [Código de error 2523](#)
- [Código de error 2502](#)
- [Código de error 2517](#)

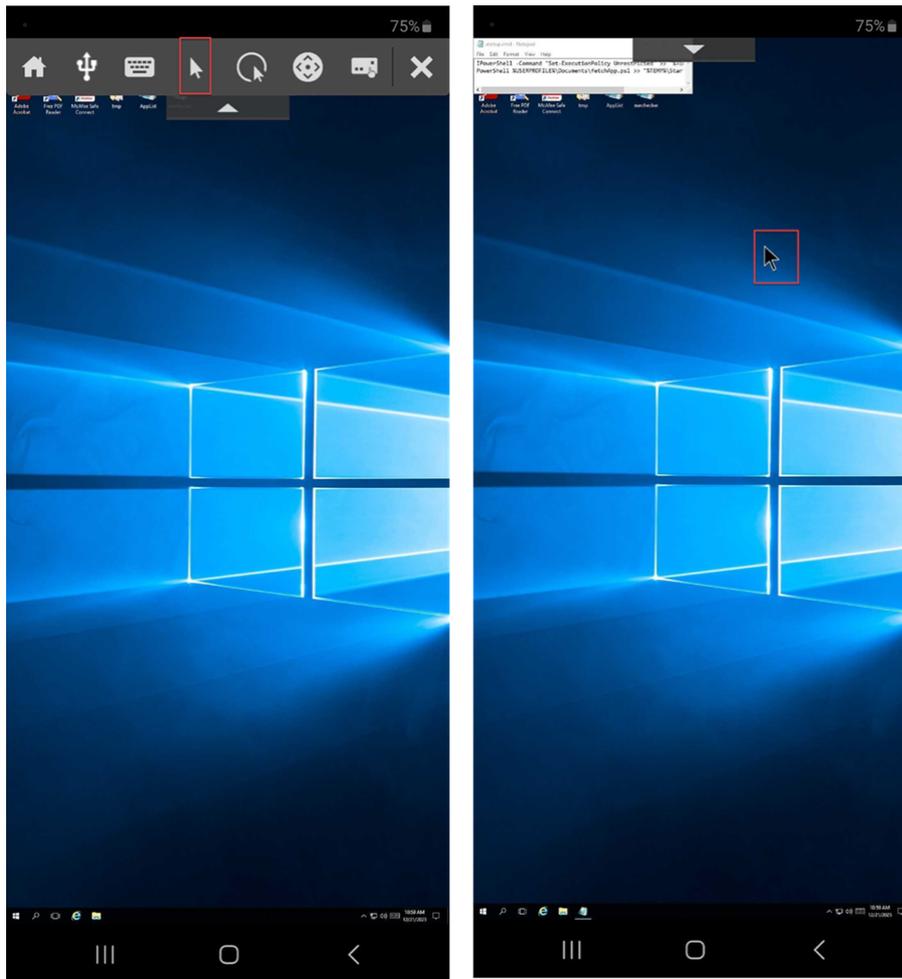
Permisos para acceder a los periféricos

Habilite los parámetros de los permisos adecuados.

Confianza en clientes selectivos Habilite los parámetros del micrófono, la ubicación y la cámara. En la aplicación Citrix Workspace, vaya a **Parámetros** > **Parámetros del almacén** y habilite los parámetros de CST para un almacén seleccionado.

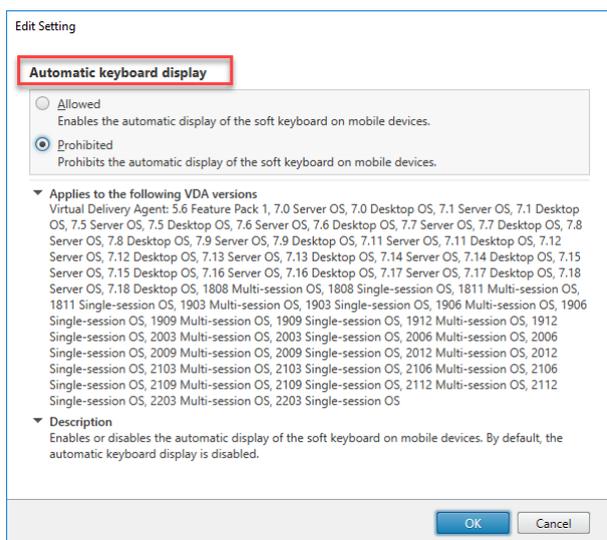


Habilitar el puntero del mouse Tras iniciar una sesión, toque la barra de herramientas y toque el icono del puntero del mouse para habilitarlo.



Habilitar teclado Si el administrador de su organización no ha habilitado la función de visualización automática del teclado de forma predeterminada, contacte con el administrador de su organización para obtener más ayuda.

Los administradores deben habilitar la directiva **Visualización automática del teclado** en el parámetro DDC.



Preguntas frecuentes

- ¿Cómo mejorar la experiencia de los usuarios de vídeo de las aplicaciones virtuales y los escritorios virtuales para dispositivos móviles o dispositivos de bajo consumo?
 - Para obtener más información, consulte el artículo de Knowledge Center [Experiencia de los usuarios de vídeo](#).
- Acceso a los recursos: ¿No puedo ver mis aplicaciones o escritorios después de iniciar sesión en la aplicación Citrix Workspace?
 - Contacte con el servicio de asistencia de su empresa o con el administrador del equipo de asistencia técnica de TI para obtener más ayuda.
- ¿Cómo solucionar problemas de conexiones lentas?
 - Siga las indicaciones de la solución temporal si tiene alguno de estos problemas:
 - conexiones lentas al sitio de Citrix Virtual Apps and Desktops
 - Faltan iconos de aplicaciones
 - Mensajes recurrentes del tipo **Error de controlador de protocolo**

Solución temporal:

- Inhabilite las propiedades del **adaptador Citrix PV Ethernet** para la interfaz de red en:
 - Servidor de Citrix Virtual Apps
 - Citrix Secure Web Gateway
 - Servidor de Interfaz Web

- Las propiedades del **adaptador Citrix PV Ethernet** incluyen (todas 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 temporal se aplica a Windows Server 2003 y 2008 de 32 bits. Este problema no afecta a Windows Server 2008 R2.

- Problema con las teclas numéricas y los caracteres especiales
 - Si las teclas numéricas o los caracteres IME chinos no funcionan correctamente, inhabilite la opción **Teclado Unicode**. Para ello, vaya a **Parámetros > Opciones de teclado** y establezca **Usar teclado Unicode** en **inhabilitado**.

Solución de problemas de códigos de error

En la tabla siguiente se muestra la lista de códigos de error y una posible solución:

Código de error	artículo de Knowledge Center
Código de error 437	https://support.citrix.com/article/CTX463401
Código de error 41E	https://support.citrix.com/article/CTX235177
Código de error 546 o 547	https://support.citrix.com/article/CTX231798
Código de error 518	https://support.citrix.com/article/CTX277571
Código de error 42B	https://support.citrix.com/article/CTX260992
Código de error 548	https://support.citrix.com/article/CTX250706 https://support.citrix.com/article/CTX578359
Dirección de servidor incorrecta + Código de error 548	https://support.citrix.com/article/CTX554245
Código de error 451	https://support.citrix.com/article/CTX256708
Error genérico	https://support.citrix.com/article/CTX219073
Pruebe a conectar de nuevo	Inhabilite la opción UDP. En la aplicación, vaya a Parámetros > Avanzados > EDT

Mensajes de error y su descripción

En la tabla siguiente se muestra la lista de errores y su descripción. La solución podría ser contactar con el [Servicio de asistencia técnica de Citrix](#) para obtener más ayuda:

Error	Descripción
SessionManager.Launch.EngineLoadFailed	El motor ICA no se pudo cargar o inicializar.
SessionManager.Launch.ConnectionFailed	El motor ICA finalizó antes de conectarse.
SessionManager.Launch.LogonFailed	Sesión desconectada sin completar el inicio de sesión
SessionManager.LeaseResolution.Failed	No se puede intentar iniciar la concesión.
SessionManager.clxmtp.SoftDeny	Error en la negociación del servicio CLXMTP del motor (denegación de software).
SessionManager.clxmtp.SoftDeny_Implicit	Error en la conexión del servicio CLXMTP del motor (denegación de software implícita).
Transport.Connect.NoCGP_Fail	Error al conectar (CGP inhabilitado).
Transport.Connect.FallbackFail	Error al conectar, probada la reserva ICA.
Transport.Connect.Fail	La conexión no está disponible.

SDK y API

December 7, 2023

Kit de desarrollo de software (SDK) para canales virtuales de Citrix

El Citrix Virtual Channel SDK admite la escritura de aplicaciones del lado del servidor y controladores del lado del cliente para otros canales virtuales que usan el protocolo ICA. Las aplicaciones de canal virtual del lado del servidor se encuentran en servidores Citrix Virtual Apps and Desktops.

Esta versión del SDK permite la escritura de canales virtuales nuevos en la aplicación Citrix Workspace para Android. Si quiere escribir controladores virtuales para otras plataformas cliente, póngase en contacto con el equipo de Asistencia técnica de Citrix.

El Virtual Channel SDK ofrece:

- Las interfaces de Citrix Android Virtual Driver AIDL: **IVCService.aidl** e **IVCCallback.aidl**, que se usan con las funciones de canal virtual en el SDK de WFAPI (Citrix Server API SDK) para crear canales virtuales.
- Una clase auxiliar **Marshall.java** diseñada para facilitar la escritura de sus propios canales virtuales.
- Código fuente operacional de tres ejemplos de programas de canales virtuales, que demuestran varias técnicas de programación.

El Virtual Channel SDK requiere el SDK de WFAPI para escribir la parte del lado del servidor del canal virtual. Para obtener más información sobre la documentación del SDK, consulte [Citrix Virtual Channel SDK para la aplicación Citrix Workspace para Android](#).

Elementos retirados

June 26, 2024

Los anuncios de este artículo le avisan con antelación de las plataformas, los productos Citrix y las funciones que se están retirando progresivamente. Con estos anuncios, puede tomar decisiones comerciales oportunas.

Citrix analiza el uso que hacen los clientes de una función que está por retirar y los comentarios que tengan sobre la eliminación de la función para determinar cuándo retirarla. Estos anuncios están sujetos a cambios en las versiones posteriores y es posible que no contengan todas las funciones o funciones retiradas.

Los elementos retirados no se quitan inmediatamente. Citrix sigue dándoles asistencia en esta versión, pero en el futuro se retirarán.

Elemento	Retirada anunciada en la versión de la aplicación Citrix Workspace	Eliminado en la versión de la aplicación Citrix Workspace	Alternativa
Sistemas operativos Android anteriores a la versión 12.0	24.5.0	24.7.0	Es compatible con Android 12.0 versiones posteriores
Compatibilidad con los protocolos TLS 1.0 y TLS 1.1	24.4.0	Versión futura	Protocolo TLS 1.2 o TLS 1.3

Elemento	Retirada anunciada en la versión de la aplicación Citrix Workspace	Eliminado en la versión de la aplicación Citrix Workspace	Alternativa
Servicios XenApp (también conocidos como PNAgent)	24.3.5	Versión futura	En la aplicación Workspace, conéctese a los almacenes con la URL de almacén en lugar de la URL de los servicios XenApp
Sistemas operativos Android anteriores a la versión 9.0	24.1.0	24.3.0	Es compatible con Android 9.0 versiones posteriores
Aplicación Citrix Workspace para Android en ChromeOS	23.8.0	23.12.0	Para usar la aplicación Citrix Workspace en ChromeOS, instale la extensión .
Workspace con funciones inteligentes	-	23.2.0	-
Compatibilidad con Android Enterprise	-	23.2.0	-
Experiencia de Workspace en dispositivos móviles	-	23.2.0	-
Autenticación con RSA SecurID	2008	-	-
Sistemas operativos Android anteriores a la versión 7.0	1903	1906	Se admiten la versión 7.0 (Nougat) y posteriores



© 2024 Cloud Software Group, Inc. All rights reserved. Cloud Software Group, the Cloud Software Group logo, and other marks appearing herein are property of Cloud Software Group, Inc. and/or one or more of its subsidiaries, and may be registered with the U.S. Patent and Trademark Office and in other countries. All other marks are the property of their respective owner(s).