Citrix Workspace app 2203.1 LTSR for Windows

Copyright © 1997–2026. Citrix Systems, Inc. All Rights Reserved.

Contents

About this release 2

Fixed issues 2

Known Issues 20

Third party notices 21

System requirements and compatibility 21

Install and Uninstall 29

Deploy 42

Update 50

Get started 57

Configure 75

Configuring single sign-on to Citrix Workspace app 166

Authenticate 170

Secure communications 187

Storebrowse 197

Citrix Workspace app Desktop Lock 206

Software Development Kit (SDK) and API 211

ICA® Settings Reference 213

© 1997–2026 Citrix Systems, Inc. All rights reserved.

About this release

September 7, 2025

What's new in 2203.1 LTSR

Citrix Workspace app 2203.1 CU6 Hotfix 2 for Windows is the most recent update to the 2203.1 Long Term Service Release (LTSR).

> Note:
>
> This release supports features that were included in Citrix Workspace app 2002 for Windows to Citrix Workspace app 2202 for Windows, except the features pertaining to components mentioned in the Notable exclusions section.

Audio redirection enhancement

Improved audio echo cancellation support for all audio codecs including Adaptive audio and all legacy audio codecs.

Microsoft Teams optimization

- **App Protection and Microsoft Teams enhancement**: Microsoft Teams supports incoming video and screen sharing when Citrix Workspace app for Windows with App Protection enabled is on **Desktop Viewer** mode only. Published apps in seamless mode don't render incoming video and screen sharing.

Service continuity

Service continuity removes or minimizes the dependency on the availability of components that are involved in the connection process. Users can launch their virtual apps and desktops regardless of the health status of the cloud services.

For more information, see Service continuity section in the Citrix Workspace documentation.

Fixed issues

September 7, 2025

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Citrix Workspace app 2203.1 LTSR CU6 Hotfix 2 for Windows

Compared to: Citrix Workspace app 2203.1 LTSR CU6 Hotfix 1

Security issues

This fix addresses a security issue for CVE-2024-6286. For more information, see Knowledge Center article CTX678036. [CVADHELP-25801].

Citrix Workspace app 2203.1 LTSR CU6 Hotfix 1 for Windows

Compared to: Citrix Workspace app 2203.1 LTSR CU6

- You might experience launch failure as `wfica32.exe` stops responding when using Citrix Workspace app for Windows version 2203.1 LTSR CU6. [CVADHELP-24770]
- Custom virtual driver keys might not be retained on uninstalling Citrix Workspace app for Windows. [CVADHELP-24513]

Citrix Workspace app 2203.1 LTSR CU6 for Windows

Compared to: Citrix Workspace app 2203.1 LTSR CU5

Session/ Connection

- If connection lease was enabled for cloud store, Citrix Workspace app for Windows starts sessions successfully even after the session limit is exceeded. [CVADHELP-23771]
- qlaunch might fail for the first time when `selfservicemode` is set to false. [CVADHELP-24414]
- If WPAD proxy setting are configured on a client machine when session reliability takes place, `wfica32.exe` process stops responding. [CVADHELP-23873]
- If the ICA® file or the folder where the ICA file is present is named with Unicode characters, you might fail to start sessions. This issue occurs only in hybrid launch. [CVADHELP-23843]
- Citrix Workspace app for Windows 2212 version might fail to follow the conditions set in the proxy PAC file. [CVADHELP-22503]

© 1997–2026 Citrix Systems, Inc. All rights reserved.

User Experience

- When you change the store configuration using the Group Policy Object Template or using the command-line, you might notice a white screen.[CVADHELP-23801]
- The refresh functionality might fail with custom domain cloud stores. [CVADHELP-23733]
- When multiple accounts are configured through GPO and you activate any disabled account, Citrix Workspace app always switches to all accounts view instead of the selected single account. [CVADHELP-24018]
- If you have Google Japanese IME enabled with Citrix IME Best experience mode, you might not be able to delete textboxes in PowerPoint using the **delete** key. [CVADHELP-23605]
- If a full screen HDX™ session is on focus, and endpoint is locked using `Ctrl`+`Alt`+`Del`, users might be unable to type anything after unlocking. [CVADHELP-24512]
- You might notice that the app opens even after closing Citrix Workspace app when you highlight an app using the tab, then Citrix Workspace app, and then press **Enter**. [CVADHELP-22700]

System exceptions

- On upgrading the VDA to Citrix Virtual Apps and Desktops 2308 or later, Citrix Workspace app might stop responding when launching seamless published application windows. [CVADHELP-23976]
- In Non English client machines, if the published application has an Unicode title, `wfica32.exe` is not compatible with the Analytics components.[CVADHELP-24471]

Seamless Windows

- If you move an application to another monitor and minimize it, the application might not open properly in the maximized view. You can try closing the application and opening it again. [CVADHELP-23703]

Installing, Uninstalling, Upgrading

- Custom virtual driver keys might not be retained on uninstalling Citrix Workspace app. [CVADHELP-24513]

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Client device Issues

- Any Composite device like **Bloomberg Keyboard 5 Biometric Module** might fail to connect automatically even when automatic redirection of client USB devices is on. [CVADHELP-22673]

User Interface

- Citrix Workspace might fail to enumerate the published resources for a brief period of time when connecting to a Global server load balancing (GSLB) URL. This issue occurs when the established StoreFront server encounters any issues that cause a GSLB controlled Virtual IP (VIP) address change in the endpoint. [CVADHELP-22467]
- You might fail to add a store when the top-level-domain (TLD) of the store URL is less than two characters or when there is no TLD. [CVADHELP-23973]

Logon/Authentication

- Citrix Workspace app with SAML2 and FAS authentication might fail to sign in automatically on session unlock even when the **WSCReconnectMode** for Workspace control is set to **reconnect on Windows sign-on** and the **Silent authentication to Citrix Workspace** policy is enabled. [CVADHELP-23018]

Citrix Workspace app 2203.1 LTSR CU5 for Windows

Compared to: Citrix Workspace app 2203.1 LTSR CU4

HDX Plug and Play

- Setting new and existing USB devices to deny the following prompt might still appear:

  Citrix Workspace has detected one or more devices connected to your computer. To connect the devices to your session, click here.

  [CVADHELP-23506]

Installing, Uninstalling, Upgrading

- After restarting a client endpoint, the periodic auto update check before you sign in might fail. [CVADHELP-23054]
- After Citrix Workspace app installation completes, you might get a fatal error prompt when configuring a store using GPO or the command line. [CVADHELP-23345]

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Keyboard

- In a double-hop scenario, the **Alt+Tab** key might not work on macOS clients. [CVADHELP-23085]

Session/Connection

- When you connect to a desktop using Cache Redirection mode and if ADC High Availability fails, you might not be able to reconnect to a desktop using Cache Redirection mode. [CVADHELP-22881]
- You might fail to start Citrix Workspace app using the API from ICO SDK after upgrading to a newer version. [CVADHELP-22940]
- When the self-service mode is set to **False** and the desktop lock feature is enabled, you might fail to add a store and might fail to start a desktop. [CVADHELP-23052]
- Published application content might appear frozen for some users randomly. The issue occurs when the TCP connection is established before the UDP connection and EDT MTU discovery isn't triggered when switching over from TDP to UDP. [CVADHELP-23253]
- When you log off from an endpoint, the wfica32.exe process might become unresponsive and block the logoff. [CVADHELP-23617]

User Experience

- You might not be able to sign in to Citrix Workspace app using a single sign-on or might not see the authentication prompt in cloud stores. The issue occurs when the account is configured through the GPO or command line for the first time and when the self-service mode is set to false and the Silent authentication to Citrix Workspace policy is enabled. [CVADHELP-22641]
- Citrix VPN might log off when you log off from Citrix Workspace app even when the VPN has been decoupled with the **DisableIconHide** registry value, which is set to **1**. [CVADHELP-22916]
- The store account addition might take a long time, or it might fail on the endpoint with no internet access or when the Global App Config Server is unreachable. [CVADHELP-22999]
- The SelfService executable might run even though no account is added in the Citrix Workspace app. [CVADHELP-23124]

User Interface

- When you open a published desktop with Unicode characters, the Desktop Viewer name might appear garbled. The issue occurs only with Internet Explorer (IE) mode in Microsoft Edge. [CVADHELP-22925]

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Citrix Workspace app 2203.1 LTSR CU4 for Windows

Compared to: Citrix Workspace app 2203.1 LTSR CU3

Content Redirection

- With the fix, you can prevent ping check and allow auto redirect URL in a host to client redirection.
    - To prevent ping check in a host to client redirection, set the following registry key:

      HKEY_LOCAL_MACHINE/SOFTWARE/Wow6432Node/Citrix/ICA Client/SFTA

      Name: OverridePingCheck

      Type: REG_DWORD

      Value: 1
    - To allow auto redirect URL in host to client redirection, set the following registry key:

      HKEY_LOCAL_MACHINE/SOFTWARE/Wow6432Node/Citrix/ICA Client/SFTA

      Name: OverridePreventAutoRedirect

      Type: REGREG_DWORD

      Value: 1

  [CVADHELP-22824]

Installing, Uninstalling, Upgrading

- Attempts to upgrade Citrix Workspace app for Windows version 1912 CU2 or earlier installed with the **Enable app protection** option might fail with this error message:

  Service 'AppProtection Service'(entryprotectsvc) failed to start. Verify that you have sufficient privileges to start system services.

  [CVADHELP-22404]
- The `CitrixReceiverUpdater.exe` command might fail to update **Autoupdate** settings like **AutoUpdateStream**, if the auto update settings were changed earlier from **Advance Preferences > Citrix Workspaces Updates**. [CVADHELP-22840]

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Session/Connection

- There might be a delay in adding a store due to certificate revocation check requests for the store's certificate. As a workaround, you can skip checking certificate revocation using the following registry:

  - HKEY_LOCAL_MACHINE/Software/wow6432node/Citrix/Receiver

    Name: SkipStoreCertificateRevocationCheck

    Type: DWORD

    Value: 1

    Or

  - HKEY_CURRENT_USER/Software/Citrix/Receiver

    Name: SkipStoreCertificateRevocationCheck

    Type: DWORD

    Value: 1

  [CVADHELP-21931]

- The session might disconnect if you click the **Desktop Viewer** and resize a published desktop continuously. [CVADHELP-22063]
- Attempts to reconnect to certain non-English language desktop versions using Auto Client Reconnect might fail with an error message. [CVADHELP-22507]
- Thinwire full-screen H.265 might fall back to H.264 with Citrix Workspace app 2203.1 LTSR CU3 for Windows. [CVADHELP-22919]

System Exceptions

- The msedgewebview2.exe process can cause high CPU usage when selfservice is running. [CVADHELP-21610]
- The wfica32.exe process might exit unexpectedly during a user session with HDX webcam redirection. [CVADHELP-22249]
- The wfica32.exe process might exit unexpectedly when the session is shutting down. [CVADHELP-22329]

© 1997–2026 Citrix Systems, Inc. All rights reserved.

User Experience

- The desktop shortcut settings per application might take high precedence by default. Also, setting the desktop shortcuts to **False** on the client side might not take effect. With this fix and by setting the following registry key, the client-side desktop shortcut settings override the desktop shortcut settings per application.

  Set the following registry key to override the desktop shortcut settings:

  HKEY_LOCAL_MACHINE\Software\Citrix\Dazzle

  Name: ProviderSettingOverride

  Type: REG_SZ

  Value: True

  [CVADHELP-15550]

- In high latency environments, a jittery movement might be observed in the mouse cursor on Citrix Workspace app when the **Use relative mouse** setting is enabled.

  To enable the fix, modify the default.ica file in StoreFront at C:\inetpub\wwwroot\Citrix\Store\App_Data\defa

  Add `RelMouseSyncTimeout=xxx(min 10 to max 1000)` to the `[WFClient]` section.

  Or

  Set the following registry key on the endpoint:

  HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\Citrix\ICA Client\Engine\Configuration\Advanced\Mod

  Name: RelMouseSyncTimeout

  Type: STRING

  Value: The minimum value is 10 and the maximum value is 1000

  [CVADHELP-21829]

- Attempts to copy and paste .msg files from local Microsoft Outlook to a published explorer might fail. [CVADHELP-22542]

User Interface

- When you sign in to the Citrix Workspace app, apps and desktops corresponding to multiple accounts configured through GPO or the command line might not be displayed. This issue occurs when the registry key value of `CurrentAccount` is set to `AllAccount` at Computer\HKEY_LOCAL_MACHINE\Software\wow6432Node\Citrix\Dazzle. [CVADHELP-21124]

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- You might get the following error message when the **AllowAddStore** parameter is set to **N** value and an HTTP store is added using a Group Policy Object (GPO) or command line interface:

  Unable to connect to the server.

  [CVADHELP-22184]
- For cloud stores, you might fail to add an account using redirect URLs. [CVADHELP-22438]
- You might see a store name different than the name that you've provided on Citrix Workspace app. [CVADHELP-22452]
- After upgrading to Citrix Workspace app for Windows 2203 LTSR, you might see a white screen. This issue occurs when you add and configure a store for the first time and simultaneously refresh and open the self-service UI. [CVADHELP-22696]

Citrix Workspace app 2203.1 LTSR CU3 for Windows

Compared to: Citrix Workspace app 2203.1 LTSR CU2

Client Device Issues

- If the Generic USB **RemoveOnLock** policy value contains upper-case letters, the policy might fail to disconnect the USB device (for example, Signature pads) in a locked client. [CVADHELP-21492]

HDX Realtime

- When a Microsoft Outlook reminder appears during a Microsoft Teams call, a black square is displayed on the shared screen of Microsoft Teams. [CVADHELP-19222]

Installing, Uninstalling, Upgrading

- The Local App Access feature might fail to work for user devices installed with the Italian language operating system. [CVADHELP-21986]
- Attempts to install Citrix Workspace app might fail on Windows Server 2012 R2. For more information, see Knowledge Center article CTX477888. [CVADHELP-22116]

Keyboard

- When you press and hold the **PrtSc** key, the server-side published application might receive VK_SNAPSHOT WM_KEYUP events (screen snapshots taken) continuously. [CVADHELP-21209]

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Logon/Authentication

- With the **Selfservicemode** set to false, the stores added might not be refreshed correctly after opening Citrix Workspace app. As a result, the authentication window fails to appear. [CVADHELP-20593]
- The inactivity timeout value might not expire if you exit from the Citrix Workspace app before reaching the set time-out value. As a result, you might later be able to start Citrix Workspace app without entering any credentials. [CVADHELP-20912]
- Attempts to enumerate applications using the **storebrowse** command might fail if the Citrix Gateway URL used is `**.\storebrowse.exe -U { Username } -P { Password } -D { Domain } -M 0x2000 -E { NSG_URL }`. [CVADHELP-21910]

Seamless Windows

- In a seamless session, the mouse and keyboard of the user device might freeze intermittently, if the application disables and then enables its window in that sequence. [CVADHELP-21031]
- When you use the **Windows Aero snap** feature to move a maximized window from one monitor to a larger monitor running Windows 11, the session might disappear. [CVADHELP-21173]
- When you open a published app in seamless mode, other local or seamless apps might appear in the foreground and cover the published app. [CVADHELP-20742, CVADHELP-21277]
- A published application might open in a non-visible state when you start the application. [CVADHELP-21618]

Session/Connection

- COM port redirection might be blocked during session roaming. [CVADHELP-20959]
- With the **Use relative mouse** setting enabled in a user session, the left click might not work on the trackpad. [CVADHELP-21223]
- In an isolated environment, Citrix Workspace app might attempt to connect to the Global App Config server even if the **Global App Config Service** policy is disabled through GPO. This causes a delay while adding an account. [CVADHELP-21319]
- Citrix Analytics is unable to receive network-related metrics from end users. This issue occurs even when these prerequisites are met:
  - App or desktop sessions are in running state for more than 15 minutes using Citrix Workspace app.
  - Store or account used is CAS enabled.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

> **Note:**
>
> Network-related CAS events are not sent for browser-based launch of apps or desktops. It's sent only when you open an app or a desktop via web and from the same store that is added via native Citrix Workspace app.

[CVADHELP-21448]

- Sometimes the published apps running on a published desktop might fail to start and Citrix Workspace app becomes unresponsive. [CVADHELP-21604]
- Attempts to access Citrix Workspace app for Windows might fail when the VPN disconnects or reconnects. [CVADHELP-21662]
- The Windocker.exe process might incorrectly generate outbound network requests to multiple IP addresses. [CVADHELP-21728]
- Using auto client reconnect might delay connecting to a session. [CVADHELP-21738]
- When you attempt to configure multiple stores through a Group Policy Object (GPO) or command line, one of the stores might not be fully configured. [CVADHELP-22034]
- Citrix Analytics file download events such as file name and file path attributes might be empty. [CVADHELP-22194]

System Exceptions

- When you start a published application with the **Adaptive Audio** policy enabled, the wfica32 process might exit unexpectedly. [CVADHELP-20999]
- Some binaries of Citrix Workspace app might be unsigned resulting in security issues. [CVADHELP-21159]

User Experience

- When you minimize and maximize a desktop, the toolbar location might not be retained. [CVADHELP-21258]
- When you disconnect and reconnect to a session that is set to full-screen mode, the toolbar location might not be retained. [CVADHELP-21324]
- You might experience delay in enumerating apps and starting apps or desktops when using SSON in an environment that has no active access to external sites. This issue occurs from the Citrix Workspace app version 2210.5 onwards and from the Citrix Workspace app version 2203 CU2 onwards. [CVADHELP-21786]

© 1997–2026 Citrix Systems, Inc. All rights reserved.

User Interface

- You might fail to add a hidden store to the Citrix Workspace app. This issue occurs when you try to add Citrix Gateway FQDN that requires smartcard authentication or when the StoreFront store name has spaces, for example, `https://servername.company.com?Store Service`. [CVADHELP-21516]
- After a store is added with the store authentication token set to **true**, Citrix Workspace might become unresponsive at the white screen and the store authentication token is set to **false**. [CVADHELP-21582]
- The screen might display the authentication pop-up window on the upper left corner instead of displaying on the center. [CVADHELP-21835]
- The WebView status bar might appear at the bottom of Citrix Workspace app when you hover the mouse over any published app or desktop icon. [CVADHELP-22108]
- When you open a native Citrix Workspace app and right-click on the self-service UI, a context menu might appear. [CVADHELP-22131]

Citrix Workspace app 2203.1 LTSR CU2 for Windows

Compared to: Citrix Workspace app 2203.1 LTSR CU1

Installing, Uninstalling, Upgrading

- When you install Citrix Workspace app as a system user using certain third-party applications, incorrect error messages might appear in the installation logs. [CVADHELP-20695]

Keyboard

- On a Surface Pro device, when you choose the on-screen keyboard on the Desktop Viewer, the keyboard might not appear. [CVADHELP-20564]

Logon/Authentication

- With this fix, you can suppress the webview authentication prompt while using the single sign-on authentication.

  To enable the fix, set the following registry key:

  HKEY_LOCAL_MACHINE/SOFTWARE/Wow6432Node/Citrix/AuthManager or HKEY_CURRENT_USER/SOFTWA

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Name: HideAuthPrompt

Type: REG_SZ

Value: True

[CVADHELP-20799]

Session/Connection

- Citrix Workspace app version 2109 and later might ignore the default.ica file settings on the StoreFront server. [CVADHELP-20017]
- When you configure a default internal beacon as the StoreFront store URL (for example, `https://example.com/Citrix/Store/discovery`) in Citrix Workspace app, the HTTP HEAD requests sent to these URLs might result in 404 errors. [CVADHELP-20329]
- Attempts to start a published application through Citrix Workspace app on an endpoint with more than eight monitors might fail with the following error message:

  This version of Workspace doesn't support the selected encryption. Please contact your administrator.

  [CVADHELP-20555]
- If the browser name (BrowserName) of a published application contains multibyte characters, the application might fail to launch. The issue occurs on Internet Explorer version 11 and Microsoft Edge opened in Internet Explorer mode. [CVADHELP-20684]
- When using Citrix Workspace app for Windows 2106 or later, the Outbound ICA Proxy feature might not work. [CVADHELP-20824]
- Citrix Workspace app prompts you to select a certificate even when only one certificate exists. This issue occurs while authenticating to the Workspace (cloud) store.

  You can suppress this certificate prompt by adding the following registry:

  - On 32-bit systems:

    HKEY_LOCAL_MACHINE/SOFTWARE/Citrix/Dazzle or HKEY_CURRENT_USER/SOFTWARE/Citrix/Dazzle

    Name: SuppressCertSelectionPrompt

    Type: REG_SZ

    Value: True
  - On 64-bit systems:

    HKEY_LOCAL_MACHINE/Software/Wow6432Node/Citrix/Dazzle or HKEY_CURRENT_USER/Software/W

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Name: SuppressCertSelectionPrompt

Type: REG_SZ

Value: True

[CVADHELP-20844]

- If Client USB device redirection is disabled in an existing session and you start a new session with the redirection enabled, the redirection might not work. [CVADHELP-20858]

System Exceptions

- Citrix Authentication Manager (AuthManSvr.exe) might exit unexpectedly during logon. [CVADHELP-17233]
- The wfica32.exe process might experience an access violation and exit unexpectedly. [CVADHELP-20558]
- When you unplug an audio device, the wfica32.exe process might experience an access violation and exit unexpectedly. The issue occurs after upgrading Citrix Workspace app for Windows to version 2203.1 LTSR CU1. [CVADHELP-21123]
- The Citrix Desktop Viewer (CDViewer.exe) might exit unexpectedly when the ICA file size is 4096 bytes. [CVADHELP-21128]

User Experience

- Citrix Workspace app might display a blurred image when you press the Shift+F2 key multiple times in a user session with Desktop Viewer disabled. [CVADHELP-20467]
- When you start a VDA machine and log on to a user session for the first time, you might have to move the mouse explicitly to see the cursor. [CVADHELP-20818]
- When you start a seamless application in Windows 10 kiosk mode, the mouse cursor does not respond correctly and fonts might appear distorted. [CVADHELP-20860]

User Interface

- Citrix Workspace app might not be responsive after the launch. [CVADHELP-20317]
- Attempts to access Citrix Workspace app for Windows might fail when the VPN disconnects or reconnects [CVADHELP-20376]
- When you add two stores from the same StoreFront server via GPO, configuring the second store might fail intermittently. [CVADHELP-20655]

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- When you add a disabled store through a GPO and a different store from the same StoreFront server through a GUI, a loading screen might appear and adding an account might fail. [CVADHELP-20776]

Citrix Workspace app 2203.1 LTSR CU1 for Windows

Compared to: Citrix Workspace app 2203.1 LTSR

Content Redirection

- When Desktop Viewer is set to full-screen mode and the default browser is maximized on the endpoint device, the Bidirectional Content Redirection feature might not bring the local default web browser window to the foreground. The issue occurs with local default web browsers other than Internet Explorer. [CVADHELP-19041]

HDX RealTime

- During a peer-to-peer call with Microsoft Teams HDX optimization, app window sharing might fail to stop after a high number of start/stop sharing repetitions, and you might not be able to share the desktop screen or app window, call or receive an incoming call until you restart Citrix Workspace app. [CVADHELP-20162]

Installing, Uninstalling, Upgrading

- Citrix Workspace The updater service might fail to start resulting in installation failure. The issue occurs when the client isn't connected to the internet. [CVADHELP-19613]

Keyboard

- After launching an HDX session, when you change the foreground window to a local application window, system keys such as **Windows** and **Alt-Tab** might be handled by the Citrix session instead of the local PC desktop, though the Citrix session is running in the background. [CVADHELP-19778]

Logon/Authentication

- After you successfully log on using Citrix Workspace app, an incorrect sign-in prompt with this message might appear:

© 1997–2026 Citrix Systems, Inc. All rights reserved.

You must sign in to access Citrix Workspace.

[CVADHELP-19676]

Seamless Windows

- When you plug in or unplug a monitor, the seamless window might be positioned incorrectly. [CVADHELP-19168]

Session/Connection

- RDP sessions might fail to launch on Citrix Workspace app 1912 LTSR CU6 for Windows when smart card redirection through RDP is enabled. [CVADHELP-19430]
- When you access a VDA for the first-time using Citrix Workspace app for Windows version 2112 or later, the following security message might appear:

  An Online Application is attempting to access information on a device attached to your computer HDX File Access.

  In previous versions, this message was present only during the first access to each published resource in a Delivery Group and not every VDA.

  [CVADHELP-19636]
- Attempts to launch applications or desktops from a tablet using Citrix Workspace app might fail. The issue occurs when the client IP address can't be retrieved. [CVADHELP-19703]
- Configuring stores with geo DNS URL via Group Policy Object or command line might fail if you have set `AllowAddStore=N` during the Citrix Workspace app installation. [CVADHELP-19853]
- When using Citrix Workspace app 2204.1 or later, the session might disconnect. This issue occurs if there's a restriction to run unsigned binaries, for example, wfica.ocx. [CVADHELP-20053]

System Exceptions

- Dragging and dropping a window in an HDX session might be slow and might cause the wfica32.exe process to exit unexpectedly. [CVADHELP-19482]
- The **Applocker** rule in Group Policy Object blocks the integration of the Citrix Gateway plug-in with Citrix Workspace. As a result, several temporary files of the format VP-NXXXX.tmp are created in the temp folder. The files are created even when the registry key, HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\Secure Access Client has **DisableIconHide** value. [CVADHELP-19709]

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- This fix addresses a rare memory leak issue in the wfica32.exe process that occurs with Citrix Workspace app for Windows. [CVADHELP-19904]
- Microsoft Office applications might exit unexpectedly when the Software protection service fails to start because of faulty App Protection components. [CVADHELP-20667]

User Experience

- Dragging and dropping files from the user device to a published application might work the first time it's attempted. Subsequent attempts fail and the application does not respond. [CVADHELP-17211]
- If you drag and drop a window in an HDX session, it takes time for the window to recover and the taskbar icon to appear. [CVADHELP-19440]
- The drag and drop feature might not work when you close a dialog box using the **Esc** key in a seamless session. [CVADHELP-19604]
- When you update the Citrix Workspace app from version 2006 or earlier, the gateway and beacon configurations of the existing stores might get deleted and the same configurations are added again even when the store configurations aren't changed in the Group Policy Object. [CVADHELP-19839]
- Accessing a web store URL from Citrix Workspace app for Windows can cause the workspace window to appear in the foreground instead of the background after each refresh interval. [CVADHELP-19885]
- Citrix Workspace app might continue to send data to `https://rttf.citrix.com` even after Customer Experience Improvement Program (CEIP) is disabled. [CVADHELP-20016]

User Interface

- On Citrix Workspace app for Windows, when you add store URLs using Group Policy Object, the following error message might appear:

  Cannot connect to server.

  This issue occurs if one of the stores is disabled and isn't reachable.

  [CVADHELP-19751]

- With this fix, a sign-in page appears when you log off from Citrix Workspace app for Windows. To enable the fix, set the following registry key:

  - On 32-bit systems:

    HKEY/LOCAL/MACHINE/Software/Citrix/Dazzle

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Name: ShowSignInPageOnLogOff

Type: REG_SZ

Value: True

- On 64-bit systems:

  HKEY/LOCAL/Software/Wow6432Node/Citrix/Dazzle

  Name: ShowSignInPageOnLogOff

  Type: REG_SZ

  Value: True

[CVADHELP-19967]

- Battery status notification and automatic keyboard pop-up dialog might not appear during the session when the **Automatic keyboard display** policy is enabled on the DDC. [CVADHELP-19987]
- When you start Citrix Workspace app for the first time after adding the store URL, the following error message appears:

  Your Citrix Workspace app encountered an error while initializing Microsoft Edge WebView2. Restart your app.

  This issue occurs when you add the store URL through a GPO or command line and includes '/'after discovery, for example, `https://sales.example.com/Citrix/Store/discovery/;On;Store`.

  [CVADHELP-20214]

- The **Desktop Viewer** toolbar might not be visible when you open the virtual desktop from the custom portal stores. [CVADHELP-20253]

Citrix Workspace app 2203.1 LTSR for Windows

Session/Connection

- Citrix ADC appliance might stop responding when certain conditions are triggered from Citrix Workspace app for Windows. [HDX-39683]
- When you try to redirect to the preferred webcam as set in the Citrix Workspace app for Windows, the setting might not be executed as configured.

  With this fix, the preferred webcam is the only available webcam in the user session. This provides better control when multiple webcams are available in the user session.

  [HDX-38214]

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- With this fix, you can set **TWITaskbarGroupingMode** to **GroupNone** either in HKEY_CURRENT_USER or HKEY_LOCAL_MACHINE. The **TWITaskbarGroupingMode** key is available under, for example, HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\ICA Client\Engine\Lockdown Profiles\All Regions\Lockdown\Virtual Channels\Seamless Windows. [CVADHELP-19106]
- Attempts to add Citrix Gateway URL might fail intermittently with the following error message:

  Authentication Service cannot be contacted.

  [CVADHELP-19415]

Known Issues

September 7, 2025

Known issues in 2203.1 LTSR CU6

No new known issues have been observed in this release.

Known issues in 2203.1 LTSR CU5

No new known issues have been observed in this release.

Known issues in 2203.1 LTSR CU4

- You might fail to start sessions if the ICA file or the folder where the ICA file is downloaded is named with Unicode or non-English characters. This issue occurs only when you access and authenticate a store using a browser and then start any app or desktop using native Citrix Workspace app. [CVADHELP-23843]

Known issues in 2203.1 LTSR CU3

- Thinwire full-screen H.265 might fall back to H.264 with Citrix Workspace app 2203.1 LTSR CU3 for Windows. [CVADHELP-22919]

Known issues in 2203.1 LTSR CU2

No new known issues have been observed in this release.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Known issues in 2203.1 LTSR CU1

No new known issues have been observed in this release.

Known issues in 2203.1 LTSR

- Citrix Workspace app for Windows installation in offline mode might fail when installer can't find Microsoft Edge WebView2 on your system.

  As a workaround install **MicrosoftEdgeWebView2RuntimeInstallerX86.exe** as an administrator and then try to install Citrix Workspace app for Windows.

  [RFWIN-26329]

- Battery status notification and automatic keyboard pop-up dialog might not appear during the session when **Automatic keyboard display** policy is enabled on the DDC. [HDX-39558]
- When you plug-in an USB device or access files, Citrix Workspace app might show legacy **Citrix Workspace - Security Warning** dialog. [LCM-10369]

Third party notices

October 7, 2023

Citrix Workspace app 2203.1 LTSR for Windows might include third party software licensed under the terms defined in the following document:

Citrix Workspace app for Windows Third-Party Notices (PDF Download)

System requirements and compatibility

September 7, 2025

Requirements

Hardware requirements

- Minimum 1 GB RAM.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- The following table provides details on the required disk space to install the Citrix Workspace app.

Installation type	Required disk space
Fresh installation	572 MB
Upgrade	350 MB

> **Note:**
>
> - The installer does the check on the disk space only after extracting the installation package.
> - When the system is low on disk space during a silent installation, the dialog does not appear but the error message is recorded in the `CTXInstall\\_TrolleyExpress-\*.log`.

Software requirements

- Microsoft Edge WebView2 Runtime
- .NET 4.8
- Latest version of Microsoft Visual C++ Redistributable

Microsoft Edge WebView2 requirements The following table lists the minimum and maximum supported Microsoft Edge WebView2 Runtime versions for different Windows operating systems:

Operating system version	Minimum required Microsoft Edge WebView2 Runtime version	Maximum supported Microsoft Edge WebView2 Runtime version
Windows 10 and Windows 11	92	Not applicable (supports the latest version)
Windows Server 2012R2	92	109
Windows Server 2016, 2019, and 2022	92	Not applicable (supports the latest version)

- Citrix Workspace app is packaged with the Evergreen Bootstrapper version of Microsoft Edge WebView2 Runtime.
- Citrix Workspace app installer can install Microsoft Edge WebView2 Runtime during the Citrix Workspace app installation. However, for this installation, you must be connected to an internet.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Alternatively, you can install the suitable offline Microsoft Edge WebView2 Runtime Evergreen Standalone Installer package before installing Citrix Workspace app.

- The device must have access to the following URLs:
  - `https://*.dl.delivery.mp.microsoft.com` to download Microsoft Edge WebView2 Runtime during the Citrix Workspace app installation. For more information, see Allow list for Microsoft Edge endpoints.
  - `https://msedge.api.cdp.microsoft.com` to check for Microsoft Edge WebView2 Runtime update
- To manage Microsoft Edge WebView2 Runtime auto-update, see Update policies in the Microsoft documentation. For example, auto-update is useful in non-persistent virtual desktops where the desktops are reverted to their original state when a user signs out.

> **Note:**
>
> When you try to install or upgrade Citrix Workspace app with non-administrator privileges and Microsoft Edge WebView2 Runtime isn't present, the installation stops with the following message:
>
> 'You must be logged on as an administrator to install the following prerequisite packages:
>
> Edge Webview 2 Runtime'

.Net requirements Citrix Workspace app requires .NET 4.8. It allows you to subscribe to and launch the apps and desktops from the Citrix Workspace app user interface or command line.

When you try to install or upgrade to Citrix Workspace app 1904 or later and the requisite .NET Framework version isn't available on your Windows system, the Citrix Workspace app installer downloads and installs the required .NET Framework version.

> **Note:**
>
> - The installation fails when you try to install or upgrade Citrix Workspace app with non-administrator privileges and .NET Framework 4.8 or greater isn't present on the system.
> - **You must be connected to the internet to download and install .NET Framework. If not, the administrator can install these requirements using a deployment method, for example, SCCM.**

Microsoft Visual C++ Redistributable requirements Citrix Workspace app requires the latest version of Microsoft Visual C++ Redistributable.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

> **Note:**
>
> Citrix® recommends that you use the latest version of Microsoft Visual C++ Redistributable. Otherwise, a restart prompt might appear during an upgrade.

Starting with Version 1904, Microsoft Visual C++ Redistributable installer is packaged with the Citrix Workspace app installer. During Citrix Workspace app installation, the installer checks whether the Microsoft Visual C++ Redistributable package is present on the system and installs it if necessary.

> **Note:**
>
> If Microsoft Visual C++ Redistributable package doesn't exist on your system, Citrix Workspace app installation with non-administrator privileges might fail.

Only an administrator can install the Microsoft Visual C++ Redistributable package.

Compatibility matrix

Citrix Workspace app is compatible with all the currently supported versions of Citrix Virtual Apps and Desktops, Citrix DaaS (formerly Citrix Virtual Apps and Desktops service) and Citrix Gateway as listed in the Citrix Product Lifecycle Matrix.

Citrix Workspace app for Windows is compatible with the following Windows operating systems:

> **Note:**
>
> - Citrix Workspace app 2203.1 LTSR for Windows is the last release to support Windows Server 2012 R2 operating system.
> - Citrix Workspace app 2203.1 LTSR for Windows is not supported on Windows 7 and Windows 8.1.
> - The Citrix Gateway End-Point Analysis Plug-in (EPA) is supported on Citrix Workspace. On the native Citrix Workspace app, it's supported only when using nFactor authentication. For more information, see Configure pre-auth and post-auth EPA scan as a factor in nFactor authentication in the Citrix ADC documentation.

Operating system
Windows 11
Windows 10 Enterprise (32-bit and 64-bit Editions). For more information about compatible Windows 10 versions, see Windows 10 Compatibility with Citrix Workspace app for Windows.
Windows 10 Enterprise (LTSC 2021) support from Version 2203.1 LTSR CU1 and later

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Operating system
Windows 10 Enterprise (2016 LTSB 1607, LTSC 2019)
Windows 10 (Home edition*, Pro)
Windows Server 2022
Windows Server 2019
Windows Server 2016

*No support for domain pass-through authentication, Desktop Lock, FastConnect API, and configurations that require domain-joined Windows machine.

Windows 10 or 11 Compatibility with Citrix Workspace app for Windows

With the Windows 10 operating system, Microsoft introduced a new way to build, deploy, and service Windows: Windows as a service. New features are packaged into Feature Updates (major versions like 20H2, 21H1, 21H2). Bug fixes and security fixes are packaged into Quality Updates. These updates that can be deployed using existing management tools like SCCM.

> **Note:**
>
> - We don't recommend installing Citrix software versions that are earlier to the Semi-Annual Channel version.
> - Once a Windows 10 version reaches End of Service that version is no longer serviced or supported by the Microsoft. Citrix supports running its software only on an operating system that its manufacturer supports. For information about Windows 10 End of Service, see Microsoft's Windows Lifecycle Fact Sheet.

The following table lists the Windows 10 version number and the corresponding compatible Citrix Workspace app for Windows release/s.

Windows 10 Version number	Build number	Citrix Workspace app Version
22H2	19045	2203.1 CU1 and later
21H2	19044	2112.1 and later
21H1	19043.928	2106 and later
20H2	19042.508	2012 and later
2004	19041.113	2006.1 and later

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Windows 10 Version number	Build number	Citrix Workspace app Version
1909	18363.418	1911 and later
1903	18362.116	1909 and later
1809	17763.107	1812 and later
1803	17134.376	1808 and later

> **Note:**
>
> Windows 10 versions are compatible with mentioned Citrix Workspace app versions only. For example, Windows 10 Version 21H1 isn't compatible with the version earlier than 2106.

The following table lists the Windows 11 version number and the corresponding compatible Citrix Workspace app for Windows releases.

Windows 11 Version number	Build number	Citrix Workspace app Version
23H2	22631	2203.1 CU6
22H2	22621	2203.1 CU1 and later
21H2	22000	2203.1 and later

Validating free disk space The following table provides details on the required disk space to install the Citrix Workspace app.

Installation type	**Required disk space**
Fresh installation	572 MB
Upgrade	350 MB

Citrix Workspace app does a check for the required disk space to complete the installation. The verification is done both during a fresh installation and an upgrade.

> **Note:**
>
> - The installer does the check on the disk space only after extracting the installation package.
> - When the system is low on disk space during silent installation, the dialog does not appear but the error message is recorded in the `CTXInstall\\_TrolleyExpress-\*.log`.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Connections, Certificates, and Authentication

Connections

- HTTP store
- HTTPS store
- Citrix Gateway 10.5 and later

Certificates

> **Note:**
>
> Citrix Workspace app for Windows is digitally signed. The digital signature is time-stamped. So, the certificate is valid even after the certificate is expired.

- Private (self-signed)
- Root
- Wildcard
- Intermediate

Private (self-signed) certificates

If a private certificate exists on the remote gateway, install the root certificate of the organization's certificate authority on the user device that's accessing the Citrix resources.

> **Note:**
>
> If the remote gateway's certificate cannot be verified upon connection, an untrusted certificate warning appears. This warning appears when the root certificate is missing in the local Keystore. When a user chooses to continue through the warning, the apps are displayed but cannot be launched.

Root certificates

For domain-joined computers, you can use a Group Policy Object administrative template to distribute and trust CA certificates.

For non-domain joined computers, the organization can create a custom install package to distribute and install the CA certificate. Contact your system administrator for assistance.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Wildcard certificates

Wildcard certificates are used on a server within the same domain.

Citrix Workspace app supports wildcard certificates. Use wildcard certificates by following your organization's security policy. An alternative to wildcard certificates is a certificate with the list of server names and the Subject Alternative Name (SAN) extension. Private and public certificate authorities issue these certificates.

Intermediate certificates

If your certificate chain includes an intermediate certificate, the intermediate certificate must be appended to the Citrix Gateway server certificate. For information, see Configuring Intermediate Certificates.

Authentication

Authentication to StoreFront

	Workspace for web	StoreFront Services site (native)	StoreFront, Citrix Virtual Apps and Desktops (native), Citrix DaaS	Citrix Gateway to Workspace for web	Citrix Gateway to StoreFront Services site (native)
Anonymous	Yes	Yes			
Domain	Yes	Yes	Yes	Yes*	Yes*
Domain pass-through	Yes	Yes	Yes		
Security token				Yes*	Yes*
Two-factor authentication (domain with security token)				Yes*	Yes*
SMS				Yes*	Yes*
Smart card	Yes	Yes		Yes	Yes

© 1997–2026 Citrix Systems, Inc. All rights reserved.

	Workspace for web	StoreFront Services site (native)	StoreFront, Citrix Virtual Apps and Desktops (native), Citrix DaaS	Citrix Gateway to Workspace for web	Citrix Gateway to StoreFront Services site (native)
User certificate				Yes (Citrix Gateway plug-in)	Yes (Citrix Gateway plug-in)

* With or without the Citrix Gateway plug-in installed on the device.

> **Note:**
>
> Citrix Workspace app supports two-factor authentication (domain plus security token) using Citrix Gateway to the StoreFront native service.

Certificate revocation list

Certificate revocation list (CRL) allows Citrix Workspace app to check if the server's certificate is revoked. The certificate check improves the server's cryptographic authentication and the overall security of the TLS connection between the user device and a server.

You can enable CRL checking at several levels. For example, it's possible to configure Citrix Workspace app to check only its local certificate list or to check the local and network certificate lists. You can also configure certificate checking to allow users to log on only if all the CRLs are verified.

If you're configuring certificate checking on your local computer, exit Citrix Workspace app. Check if all the Citrix Workspace components, including the **Connection Center**, are closed.

For more information, see the Transport Layer Security section.

Install and Uninstall

September 7, 2025

You can install the Citrix Workspace app either by:

- Downloading the `CitrixWorkspaceApp.exe` installation package from the Download page or

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- From your company's download page (if available).

You can install the package using the following steps:

- Running an interactive Windows-based installation wizard. Or
- Typing the installer file name, installation commands and installation properties using the command-line interface. For information about installing Citrix Workspace app using command-line interface, see Using command-line parameters.

Installation with administrator and non-administrator privileges:

Both users and administrators can install Citrix Workspace app. Administrator privileges are required only when using pass-through authentication and Citrix Ready workspace hub with Citrix Workspace app for Windows.

The following table describes the differences when Citrix Workspace app is installed as an administrator or a user:

	Installation folder	Installation type
Administrator	C:\Program Files (x86)\Citrix\ICA Client	Per-system installation
User	%USERPROFILE%\AppData\Local\Citrix\ICA Client	Per-user installation

> **Note:**
>
> Administrators can override the user-installed instance of Citrix Workspace app and continue with the installation successfully.

Using a Windows-based installer

You can install Citrix Workspace app for Windows by manually running the `CitrixWorkspaceApp.exe` installer package, using the following methods:

- Installation media
- Network share
- Windows Explorer
- Command-line interface

By default, the installer logs are at `%temp%\CTXReceiverInstallLogs*.logs`.

1. Launch the `CitrixWorkspaceApp.exe` file and click **Start**.
2. Read and accept the EULA and continue with the installation.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

3. When installing on a domain-joined machine with administrator privileges, a single sign-on dialog appears. See Domain pass-through authentication for more information.
4. Follow the Windows-based installer to complete the installation.

When the installation is complete, Citrix Workspace app requests that you add an account. For information on how to add an account, see Add accounts or switch servers.

Using command-line parameters

You can customize the Citrix Workspace app installer by specifying different command-line options. The installer package self-extracts to the system temp directory before launching the setup program. The space requirement includes program files, user data, and temp directories after launching several applications.

To install the Citrix Workspace app using the Windows command line, launch the command prompt and type the following on a single line:

- installer file name,
- installation commands, and
- installation properties

The available installation commands and properties are as follows:

```
CitrixWorkspaceApp.exe [commands] [properties]
```

List of command-line parameters

The parameters are broadly classified as follows:

- Common parameters
- Install parameters
- HDX features parameters
- Preferences and user interface parameters
- Authentication parameters

Common parameters

- /? Or /`help` - Lists all the installation commands and properties.
- /`silent` - Disables installation dialogs and prompts during installation.
- /`noreboot` - Suppresses the prompts to reboot during installation. When you suppress the reboot prompt, USB devices that are in a suspended state aren't recognized. The USB devices are activated only after the device is restarted.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- /includeSSON - Requires you to install as an administrator. Indicates that the Citrix Workspace app is installed with the single sign-on component. See Domain pass-through authentication for more information.
- /rcu - The /rcu switch is effective only when upgrading from an unsupported version of the software. Indicates that Citrix Workspace app install or upgrade is done by uninstalling the existing version. The /rcu switch also cleans up existing or older settings.

  > **Note:**
  >
  > The /rcu switch is deprecated as of Version 1909. For more information, see Deprecation.

- /forceinstall - This switch is effective when cleaning up any existing configuration or entries of Citrix Workspace app in the system. Use this switch in the following scenarios:
  - Upgrading from an unsupported version of Citrix Workspace app version.
  - The installation or upgrade is unsuccessful.

Install parameters

/AutoUpdateCheck

Indicates that Citrix Workspace app detects when an update is available.

> **Note:**
>
> The /AutoUpdateCheck is a mandatory parameter that you must set to configure other parameters like /AutoUpdateStream, /DeferUpdateCount, /AURolloutPriority.

- Auto (default) - You're notified when an update is available. Example, CitrixWorkspaceApp.exe /AutoUpdateCheck=auto.
- Manual - You aren't notified when an update is available. Check for updates manually. Example, CitrixWorkspaceApp.exe /AutoUpdateCheck=manual.
- Disabled - Disables auto-updates. Example, CitrixWorkspaceApp.exe /AutoUpdateCheck=disabled.

/AutoUpdateStream

If you have enabled auto-update, you can choose the version you want to update. See Lifecycle Milestones for more information.

- LTSR - Auto-updates to Long Term Service Release cumulative updates only. Example, CitrixWorkspaceApp.exe /AutoUpdateStream=LTSR.
- Current - Auto-updates to the latest version of Citrix Workspace app. Example, CitrixWorkspaceApp.exe /AutoUpdateStream=Current.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

/DeferUpdateCount

Indicates the number of times that you can defer notifications when an update is available. For more information, see Citrix Workspace Updates.

- -1(default) - Allows deferring notifications any number of times. Example, `CitrixWorkspaceApp.exe /DeferUpdateCount=-1`.
- 0 - Indicates that you receive one notification (only) for every available update. Doesn't remind you again about the update. Example, `CitrixWorkspaceApp.exe /DeferUpdateCount=0`.
- Any other number 'n'- Allows deferring notifications 'n'number of times. The **Remind me later** option is displayed in the 'n'count. Example, `CitrixWorkspaceApp.exe /DeferUpdateCount=<n>`.

/AURolloutPriority

When a new version of the app is available, Citrix® rolls out the update for a specific delivery period. With this parameter, you can control at what time during the delivery period you can receive the update.

- Auto (default) - You receive the updates during the delivery period as configured by Citrix. Example, `CitrixWorkspaceApp.exe /AURolloutPriority=Auto`.
- Fast - You receive the updates at the beginning of the delivery period. Example, `CitrixWorkspaceApp.exe /AURolloutPriority=Fast`.
- Medium - You receive the updates at the mid-delivery period. Example, `CitrixWorkspaceApp.exe /AURolloutPriority=Medium`.
- Slow - You receive the updates at the end of the delivery period. Example, `CitrixWorkspaceApp.exe /AURolloutPriority=Slow`.

/includeappprotection

Provides enhanced security by restricting the ability of clients to be compromised by keylogging and screen-capturing malware.

- `CitrixWorkspaceApp.exe /includeappprotection`

See App Protection for more information.

/InstallEmbeddedBrowser

Excludes the Citrix Enterprise Browser binaries. Run the `/InstallEmbeddedBrowser=N` switch to exclude the Citrix Enterprise Browser feature.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

INSTALLDIR

Specifies the custom installation directory for Citrix Workspace app installation. The default path is `C:\Program Files\Citrix`. Example, `CitrixWorkspaceApp.exe INSTALLDIR=C:\Program Files\Citrix`.

ADDLOCAL

Installs one or more of the specified components. For example, `CitrixWorkspaceapp.exe ADDLOCAL=ReceiverInside,ICA_Client,AM,SSON,SELFSERVICE,DesktopViewer,WebHelper,WorkspaceHub,USB,AppProtection`.

> **Note:**
>
> By default, `ReceiverInside`, `ICA_Client`, and `AM` are installed when installing the Citrix Workspace app.

The `ADDLOCAL` installs one or more of the specified components.

ReceiverInside, ICA_Client, and AM are prerequisites and are installed by default when installing the Citrix Workspace app.

- ReceiverInside –Installs the Citrix Workspace app experience (required), functionality of sys tray and auto-update.
- ICA_Client –Installs the HDX™ components.
- AM –Installs Authentication Manager components.

You can also install the following modules depending on your requirement and environment:

- SSON –Installs components required for single sign-on.
- SELFSERVICE –Installs the self-service plug-in. This allows you to access virtual desktops and applications from the Citrix Workspace app window or from a command line. If SELFSERVICE is not installed, you can access the applications and desktops via the web (Receiver for Web).
- DesktopViewer –Installs Desktop Viewer for viewing virtual apps and desktops.
- WebHelper: Installs the WebHelper component. This component retrieves the ICA file from StoreFront and passes it to the HDX Engine. It also verifies the environment parameters and shares them with StoreFront. This component is used during session launch via browser.
- WorkspaceHub: Citrix Ready workspace hub component that enables Citrix Casting.
- USB –Installs USB support.
- AppProtection: Install App Protection component.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

HDX features parameters

ALLOW_BIDIRCONTENTREDIRECTION

Indicates if bidirectional content redirection between the client and the host is enabled. For more information, see the Bidirectional content redirection policy settings section in the Citrix Virtual Apps and Desktops documentation.

- 0 (default) –Indicates that the bidirectional content redirection is disabled. Example, `CitrixWorkspaceApp.exe ALLOW_BIDIRCONTENTREDIRECTION=0`.
- 1 - Indicates that the bidirectional content redirection is enabled. Example, `CitrixWorkspaceApp.exe ALLOW_BIDIRCONTENTREDIRECTION=1`.

FORCE_LAA

Indicates that Citrix Workspace app is installed with the client-side Local App Access component. Install the workspace app with administrator privileges for this component to work. See the Local App Access section in the Citrix Virtual Apps and Desktops documentation for more information.

- 0 (default)- Indicates that the Local App Access component isn't installed. Example, `CitrixWorkspaceApp.exe FORCE_LAA =0`.
- 1 - Indicates that the client-end Local App Access component is installed. Example, `CitrixWorkspaceApp.exe FORCE_LAA =1`.

LEGACYFTAICONS

Specifies if you want to display icons for documents or files that have file type association with subscribed applications.

- False (default) - Display icons for documents or files that have file type associations with subscribed applications. When set to false, the operation system generates an icon for the document that doesn't have a specific icon assigned to it. The icon generated by the operation system is a generic icon overlaid with a smaller version of the application icon. Example, `CitrixWorkspaceApp.exe LEGACYFTAICONS=False`.
- True - Doesn't display icons for documents or files that have file type associations with subscribed applications. Example, `CitrixWorkspaceApp.exe LEGACYFTAICONS=True`.

ALLOW_CLIENTHOSTEDAPPSURL

Enables the URL redirection feature on the user device. See the Local App Access section in the Citrix Virtual Apps and Desktops documentation for more information.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- 0 (default)- Disables the URL redirection feature on the user device. Example, `CitrixWorkspaceApp.exe ALLOW_CLIENTHOSTEDAPPSURL=0`.
- 1- Enables the URL redirection feature on the user devices. Example, `CitrixWorkspaceApp.exe ALLOW_CLIENTHOSTEDAPPSURL=1`.

Preference and user interface parameters

ALLOWADDSTORE

Allows you to configure the stores (HTTP or https) based on the specified parameter.

- S(default)- Allows you to add or remove secure stores only (configured with HTTPS). Example, `CitrixWorkspaceApp.exe ALLOWADDSTORE=S`.
- A –Allows you to add or remove both secure stores (HTTPS) and non-secure stores (HTTP). Not applicable if Citrix Workspace app is per-user installed. Example, `CitrixWorkspaceApp.exe ALLOWADDSTORE=A`.
- N –Never allow users to add or remove their own store. Example, `CitrixWorkspaceApp.exe ALLOWADDSTORE=N`.

ALLOWSAVEPWD

Allows you to save the store credentials locally. This parameter applies only to stores using the Citrix Workspace app protocol.

- S(default) - Allows saving the password for secure stores only (configured with HTTPS). Example, `CitrixWorkspaceApp.exe ALLOWSAVEPWD=S`.
- N - Does not allow saving the password. Example, `CitrixWorkspaceApp.exe ALLOWSAVEPWD=N`.
- A - Allows saving the password for both secure stores (HTTPS) and non-secure stores (HTTP). Example, `CitrixWorkspaceApp.exe ALLOWSAVEPWD=A`.

STARTMENUDIR

Specifies the directory for the shortcuts in the Start menu.

- `<Directory Name>` - By default, applications appear under **Start** > **All Programs**. You can specify the relative path of the shortcuts in the `\Programs` folder. For example, to place shortcuts under **Start** > **All Programs** > **Workspace**, specify `STARTMENUDIR=\Workspace`.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

DESKTOPDIR

Specifies the directory for shortcuts on the Desktop.

> **Note:**
>
> When using the DESKTOPDIR option, set the `PutShortcutsOnDesktop` key to `True`.

- `<Directory Name>` - You can specify the relative path of the shortcuts. For example, to place shortcuts under **Start > All Programs > Workspace**, specify `DESKTOPDIR=\Workspace`.

SELFSERVICEMODE

Controls access to the self-service Citrix Workspace app user interface.

- True - Indicates that the user has access to the self-service user interface. Example, `CitrixWorkspaceApp.exe SELFSERVICEMODE=True`.
- False - Indicates that the user does not have access to the self-service user interface. Example, `CitrixWorkspaceApp.exe SELFSERVICEMODE=False`.

ENABLEPRELAUNCH

Controls session pre-launch. See Application launch time for more information.

- True - Indicates that session pre-launch is enabled. Example, `CitrixWorkspaceApp.exe ENABLEPRELAUNCH=True`.
- False - Indicates that session pre-launch is disabled. Example, `CitrixWorkspaceApp.exe ENABLEPRELAUNCH=False`.

DisableSetting

Hides the **Shortcuts and Reconnect** option from being displayed in the **Advanced Preferences** sheet. See Hiding specific settings from the Advanced Preferences sheet for more information.

- 0 (default) –Displays both **Shortcuts** and **Reconnect** options in the Advanced Preferences sheet. Example, `CitrixWorkspaceApp.exe DisableSetting=0`.
- 1 –Displays only the **Reconnect** option in the Advanced Preferences sheet. Example, `CitrixWorkspaceApp.exe DisableSetting=1`.
- 2 –Displays only the **Shortcuts** option in the Advanced Preferences sheet. Example, `CitrixWorkspaceApp.exe DisableSetting=2`.
- 3 –Both **Shortcuts** and **Reconnect** options are hidden from the Advanced Preferences sheet. Example, `CitrixWorkspaceApp.exe DisableSetting=3`.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

EnableCEIP

Indicates your participation in the Customer Experience Improvement Program. See CEIP for more information.

- True (default)- Opt in to the Citrix Customer Improvement Program (CEIP). Example, `CitrixWorkspaceApp.exe EnableCEIP=True`.
- False - Opt out of the Citrix Customer Improvement Program (CEIP). Example, `CitrixWorkspaceApp.exe EnableCEIP=False`.

EnableTracing

Controls the **Always-on tracing** feature.

- True (default)- Enables the **Always-on tracing** feature. Example. `CitrixWorkspaceApp.exe EnableTracing=true`.
- False - Disables the **Always-on tracing** feature. Example, `CitrixWorkspaceApp.exe EnableTracing=false`.

CLIENT_NAME

Specifies the name used to identify the user device to the server.

- `<ClientName>` - Specifies the name used identify the user device on the server. The default name is %COMPUTERNAME%. Example, `CitrixReceiver.exe CLIENT_NAME=%COMPUTERNAME%`.

ENABLE_DYNAMIC_CLIENT_NAME

Allows the client name to be the same as the computer name. When you change the computer name, the client name changes too.

- Yes (default) –Allows the client name to be the same as the computer name. Example, `CitrixWorkspaceApp.exe ENABLE_DYNAMIC_CLIENT_NAME=Yes`.
- No - Does not allow the client name to be the same as the computer name. Specify a value for the `CLIENT_NAME` property. Example, `CitrixWorkspaceApp.exe ENABLE_DYNAMIC_CLIENT_NAME=No`.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Authentication parameters

ENABLE_SSON

Enables single sign-on when the Citrix Workspace app is installed with the `/includeSSON` command. See Domain pass-through authentication for more information.

- Yes (default) - Indicates that single sign-on is enabled. Example, `CitrixWorkspaceApp.exe ENABLE_SSON=Yes`.
- No - Indicates that single sign-on is disabled. Example, `CitrixWorkspaceApp.exe ENABLE_SSON=No`.

ENABLE_KERBEROS

Specifies whether the HDX engine must use Kerberos authentication, required only when you enable single sign-on authentication. For more information, see Domain pass-through authentication with Kerberos.

- Yes - Indicates that the HDX engine must use Kerberos authentication. Example, `CitrixWorkspaceApp.exe ENABLE_KERBEROS=Yes`.
- No - Indicates that the HDX engine doesn't use Kerberos authentication. Example, `CitrixWorkspaceApp.exe ENABLE_KERBEROS=No`.

In addition to the above properties, you can also specify the store URL that is used with the Citrix Workspace app. You can add up to 10 stores. Use the following property to do so:

```
STOREx="storename;http[s]://servername.domain/IISLocation/discovery;[On, Off]; [storedescription]"
```

Values:

- **x** - Integers 0 through 9 used to identify a store.
- **storename** - Name of the store. This value must match the name configured on the StoreFront server.
- **servername.domain** - The fully qualified domain name of the server hosting the store.
- **IISLocation** - the path to the store within IIS. The store URL must match the URL in the StoreFront provision file. The store URL is in the following format `/Citrix/store/discovery`. To get the URL, export a provisioning file from StoreFront, launch it in Notepad and copy the URL from the **Address** element.
- [On, Off] - The **Off** option lets you deliver disabled stores, giving users the choice of whether they access them. When the store status isn't specified, the default setting is **On**.
- **storedescription** - Description of the store, such as `HR App Store`.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Examples of a command-line installation

To specify the Citrix Gateway store URL:

```
CitrixWorkspaceApp.exe STORE0=HRStore;https://ag.mycompany.com#
    Storename;On;Store
```

Where, **Storename** indicates the name of the store that needs to be configured.

> **Note:**
>
> - The Citrix Gateway store URL configured using this method does not support the PNA Services Sites that are using Citrix Gateway.
> - In a multi-store setup, the Citrix Gateway store URL must be first in the list. Only one Citrix Gateway store URL configuration is allowed.

To install all components silently and specify two application stores:

```
CitrixWorkspaceApp.exe /silent
STORE0="AppStore;https://testserver.net/Citrix/MyStore/discovery;on;
HR App Store"
STORE1="BackUpAppStore;https://testserver.net/Citrix/MyBackupStore/
discovery;on;Backup HR App Store"
```

> **Note:**
>
> - It's mandatory to include `/discovery` in the store URL for successful pass-through authentication.
> - The Citrix Gateway store URL must be the first entry in the list of configured store URLs.

Reset Citrix Workspace app

Resetting Citrix Workspace app restores the default settings.

The following items are reset when you reset Citrix Workspace app:

- All the configured accounts and stores.
- Apps delivered by the self-service plug-in, their icons, and registry keys.
- File type associations created by the self-service plug-in.
- Cached files and saved passwords.
- Per-user registry settings.
- Per-machine installations, and their registry settings.
- Citrix Gateway registry settings for Citrix Workspace app.

Run the following command from the command line interface to reset the Citrix Workspace app:

© 1997–2026 Citrix Systems, Inc. All rights reserved.

```
C:\Program Files (x86)\Citrix\ICA Client\SelfServicePlugin\CleanUp.
exe"-cleanUser
```

For silent reset, use the following command:

```
C:\Program Files (x86)\Citrix\ICA Client\SelfServicePlugin\CleanUp.
exe"/silent -cleanUser
```

> **Note:**
>
> Use uppercase U in the parameter.

Resetting Citrix Workspace app does not impact the following:

- Citrix Workspace app or plug-in installation.
- Per-machine ICA® lockdown settings.
- Group policy object (GPO) administrative template configurations for Citrix Workspace app.

Uninstall

Using Windows-based uninstaller:

You can uninstall Citrix Workspace app using the Windows Programs and Features utility (Add or Remove Programs).

> **Note:**
>
> During Citrix Workspace app installation, you get a prompt to uninstall the Citrix HDX RTME package. Click **OK** to continue the uninstallation.

Using the command-line interface:

You can uninstall Citrix Workspace app, from a command line by typing the following command:

```
CitrixWorkspaceApp.exe /uninstall
```

For silent uninstallation of Citrix Workspace app, run the following switch:

```
CitrixWorkspaceApp.exe /silent /uninstall
```

> **Note:**
>
> Citrix Workspace app installer doesn't control GPO related registry keys, so they are kept after uninstallation. If you find any entries, update them using `gpedit` or delete them manually.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Deploy

October 7, 2023

You can deploy the Citrix Workspace app in the following methods:

- Use Active Directory and sample startup scripts to deploy the Citrix Workspace app for Windows. For information about Active Directory, see Using Active Directory and sample scripts.
- Before launching workspace for web, install the Citrix Workspace app for Windows. For more information, see Using workspace for web.
- Use an Electronic Software Distribution (ESD) tool like the Microsoft System Center Configuration Manager 2012 R2. For more information, see Using System Center Configuration Manager 2012 R2.
- Use Microsoft Endpoint Manager (Intune). For more information, see Deploy Citrix Workspace app in Microsoft Endpoint Manager (Intune).

Using Active Directory and sample scripts

You can use Active Directory Group Policy scripts to deploy Citrix Workspace app based on your organizational structure. Citrix recommends using the scripts rather than extracting the .msi files. For general information about startup scripts, see the Microsoft documentation.

To use the scripts with Active Directory:

1. Create the Organizational Unit (OU) for each script.
2. Create a Group Policy Object (GPO) for the newly created OU.

Edit scripts

Edit the scripts with the following parameters in the header section of each file:

- **Current Version of package** - The specified version number is validated and if it isn't presented, the deployment proceeds. For example, set `DesiredVersion= 3.3.0.XXXX` to exactly match the version specified. If you specify a partial version, for example, 3.3.0, it matches any version with that prefix (3.3.0.1111, 3.3.0.7777, and so on).
- **Package Location/Deployment directory** - This specifies the network share containing the Citrix Workspace app installer packages and is not authenticated by the script. The shared folder must have Read permission set to EVERYONE.
- **Script Logging Directory** - The network share where the install logs are copied and the ones that script didn't authenticate. The shared folder must have Read and Write permissions for EVERYONE.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- **Package Installer Command Line Options**- These command-line options are passed to the installer. For the command-line syntax, see Using command-line parameters.

Scripts

Citrix Workspace app installer includes the sample of both per-computer and per-user scripts to install and uninstall Citrix Workspace app. The scripts are present in the Citrix Workspace app for Windows Downloads page.

Deployment type	To deploy	To remove
Per-computer	CheckAndDeployWorkspacePerMachine.bat	CheckAndRemoveWorkspacePerMachine.bat
Per-user	CheckAndDeployWorkspacePerUser.bat	CheckAndRemoveWorkspacePerUser.bat

To add the startup scripts:

1. Open the Group Policy Management Console.
2. Select **Computer Configuration** or **User Configuration** > **Policies** > **Windows Settings** > **Scripts**.
3. In the right-hand pane of the Group Policy Management Console, select **Logon**.
4. Select **Show Files**, copy the appropriate script to the folder displayed, and close the dialog.
5. In the **Properties** menu, click **Add** and **Browse** to find and add the newly created script.

To deploy Citrix Workspace app for Windows:

1. Move the user devices assigned to receive this deployment to the OU that you created.
2. Reboot the user device and log on.
3. Verify that the newly installed package is listed in the **Program and Features**.

To remove Citrix Workspace app for Windows:

1. Move the user devices chosen for removal to the OU you created.
2. Reboot the user device and log on.
3. Verify that the newly installed package isn't listed in the **Program and Features**.

Using workspace for web

The workspace for a web enables you to access StoreFront stores through a browser using a web-page.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Before connecting to an app from a browser, do the following:

1. Install the Citrix Workspace app for Windows.
2. Deploy the Citrix Workspace app from workspace for web

If workspace for web detects that a compatible version of Citrix Workspace app isn't present, a prompt appears. The prompt shows that you must download and install Citrix Workspace app for Windows.

> **Note:**
>
> The workspace for the web does not support email-based account discovery.

Use the following configuration to prompt for the server address only.

1. Download `CitrixWorkspaceApp.exe` to your local computer.
2. Rename `CitrixWorkspaceApp.exe`to `CitrixWorkspaceAppWeb.exe`.
3. Deploy the renamed executable using your regular deployment method. If you use StoreFront, see Configure StoreFront using the configuration files in the StoreFront documentation.

Using System Center Configuration Manager 2012 R2

You can use Microsoft System Center Configuration Manager (SCCM) to deploy Citrix Workspace app.

You can deploy the Citrix Workspace app using the SCCM using the following four parts:

1. Adding Citrix Workspace app to the SCCM deployment
2. Adding distribution points
3. Deploying the Citrix Workspace app to the software center
4. Creating Device Collections

Adding Citrix Workspace app to the SCCM deployment

1. Copy the downloaded Citrix Workspace app installation folder to a folder on the Configuration Manager server and launch the Configuration Manager console.
2. Select **Software Library** > **Application Management**. Right-click **Application** and click **Create Application**.
   The Create Application wizard appears.
3. In the **General** pane, select **Manually specify the application information** and click **Next**.
4. In the **General Information** pane, specify the application information, such as **Name**, **Manufacturer**, **Software version**.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

5. In the **Application Catalog** wizard, specify additional information such as Language, Application name, User category and so on and click **Next**.

   > **Note:**
   >
   > Users can see the information that you specify here.

6. In the **Deployment Type** pane, click **Add** to configure the deployment type for Citrix Workspace app setup.

   The Create Deployment Type wizard appears.

7. In the **General** pane: Set the deployment type to Windows Installer (*.msi file), select **Manually specify the deployment type information**, and click **Next**.

8. In the **General Information** pane: Specify deployment type details (For example: Workspace Deployment) and click **Next**.

9. In the **Content** pane:

   a) Provide the path where the Citrix Workspace app setup file is present. For example: Tools on SCCM server.
   b) Specify **Installation program** as one of the following:
      - `CitrixWorkspaceApp.exe /silent` for default silent installation.
      - `CitrixWorkspaceApp.exe /silent /includeSSON` to enable domain pass-through.
      - `CitrixWorkspaceApp.exe /silent SELFSERVICEMODE=false` to install Citrix Workspace app in non-Self Service Mode.
   c) Specify **Uninstall program** as `CitrixWorkspaceApp.exe /silent /uninstall` (to enable uninstallation through SCCM).

10. In the **Detection Method** pane: Select **Configure rules to detect the presence of this deployment type** and click **Add Clause**.
    The Detection Rule dialog appears.

    - Set **Setting Type** to File System.
    - Under **Specify the file or folder to detect the application**, set the following:
      - **Type** –From the drop-down menu, select **File**.
      - **Path** –`%ProgramFiles(x86)%\Citrix\ICA Client\Receiver\`
      - **File or folder name** –`receiver.exe`
      - **Property** –From the drop-down menu, select **Version**
      - **Operator** - From the drop-down menu, select **Greater than or equal to**
      - **Value** - Type **4.3.0.65534**

© 1997–2026 Citrix Systems, Inc. All rights reserved.

> **Note:**
>
> This rule combination applies to Citrix Workspace app for Windows upgrades as well.

11. In the **User Experience** pane, set:
    - **Installation behavior** - Install for system
    - **Logon requirement** - Whether a user is logged on
    - **Installation program visibility** - Normal

    Click **Next**.

> **Note:**
>
> Do not specify any requirements and dependencies for this deployment type.

12. In the **Summary pane**, verify the settings for this deployment type. Click **Next**.

    A success message appears.

13. In the **Completion pane**, a new deployment type (Workspace Deployment) is listed under the **Deployment types**.
14. Click **Next** and click **Close**.

Add distribution points

1. Right-click Citrix Workspace app in the **Configuration Manager** console and select **Distribute Content**.

   The Distribute Content wizard appears.

2. In the Content Distribution pane, click **Add > Distribution Points**.

   The Add Distribution Points dialog appears.

3. Browse to the SCCM server where the content is available and clicks **OK**.

   In the Completion pane, a success message appears

4. Click **Close**.

Deploy Citrix Workspace app to the software center

1. Right-click Citrix Workspace app in the Configuration Manager console select **Deploy**.

   The Deploy Software wizard appears.

2. Select **Browse** against Collection (can be Device Collection or User Collection) where the application is to be deployed and click **Next**.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

3. In the **Deployment Settings** pane, set **Action** to Install and **Purpose** to Required (enables unattended installation). Click **Next**.
4. In the **Scheduling** pane, specify the schedule to deploy the software on target devices.
5. In the **User Experience** pane, set the **User notifications** behavior; select **Commit changes at deadline or during a maintenance window (requires restart)** and click **Next** to complete the Deploy Software wizard.

In the **Completion** pane, a success message appears.

Reboot the target endpoint devices (required only to start installation immediately).

On endpoint devices, Citrix Workspace app is visible in the Software Center under **Available Software**. Installation is triggered automatically based on the configured schedule. You can also schedule or install on demand. The installation status is displayed in the **Software Center** after the installation starts.

Creating device collections

1. Launch the **Configuration Manager** console and click **Assets and Compliance** > **Overview** > **Devices**.
2. Right-click **Device Collections** and select **Create Device Collection**.

   The **Create Device Collection** wizard appears.
3. In the **General** pane, type the **Name** for the device and click **Browse** for Limiting collection.

   This determines the scope of devices, which can be one the default **Device Collections** created by SCCM.
   Click **Next**.
4. In the **Membership Rules** pane, click **Add Rule** for filtering the devices.

   The **Create Direct Membership Rule** wizard appears.

   - In the **Search for Resources** pane, select the **Attribute name** based on the devices you want to filter and provide the Value for Attribute name to select the devices.
5. Click **Next**. In the Select Resources pane, select the devices that are required to be part of the device collection.

   In the Completion pane, a success message appears.
6. Click **Close**.
7. In the Membership rules pane, a new rule is listed under Click Next.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

8. In the Completion pane, a success message appears. Click **Close** to complete the **Create Device Collection** wizard.

   The new device collection is listed in **Device Collections**. The new device collection is a part of the Device Collections while browsing in the **Deploy Software** wizard.

> **Note:**
>
> Configuring Citrix Workspace app using SCCM might fail when the **MSIRESTARTMANAGERCONTROL** attribute is set to **False**.
> As per our analysis, Citrix Workspace app for Windows is not the cause of this failure. Also, retrying might yield successful deployment.

Deploy Citrix Workspace app in Microsoft Endpoint Manager (Intune)

To deploy Citrix Workspace app –native Win 32 app in Microsoft Endpoint Manager (Intune), do the following:

1. Create the following folders:
   - A folder to store all the source files required for the installation, for example, `C:\CitrixWorkspace_Executable`.
   - A folder for the output file. Output files are in `.intunewin` file, for example, `C:\Intune_CitrixWorkspaceApp`.
   - A folder for the Microsoft Win32 Content Prep Tool, for example, `C:\Intune_WinAppTool`. This tool helps to convert the installation files into the `.intunewin` format. You can download the packaging tool from Microsoft-Win32-Content-Prep-Tool.
2. Convert all the source files that are needed for the installation to a `.intunewin` file:
   a) Launch the command prompt and go to the folder, where the Microsoft Win32 Content Prep Tool exists, for example, `C:\Intune_WinAppTool`.
   b) Run the `IntuneWinAppUtil.exe` command.
   c) On the prompt, enter the following information:
      - **Source folder**: `C:\CitrixWorkspace_Executable`
      - **Setup file**: `CitrixWorkspaceApp.exe`
      - **Output folder**: `C:\Intune_CitrixWorkspaceApp`

      The `.intunewin` file is created.
3. Add the package to Microsoft Endpoint Manager (Intune):
   a) Open the Microsoft Endpoint Manager (Intune) console: `https://endpoint.microsoft.com/#home`.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

> **Note:**
>
> The following instruction can be performed only on https://endpoint.microsoft.com/#home. You can also add the package through https://portal.azure.com.

b) Click **Apps** > **Windows app** and then click **+Add**.

c) Select **Windows app (Win 32)** from the **App type** drop-down list.

d) Click **App package file**, locate the CitrixWorkspaceApp.intunewin file, and then click **OK**.

e) Click **App information** and fill in the mandatory information, Name, Description, and Publisher and then click **OK**.

f) Click **Program**, enter the following information, and click **OK**:

- Install command: `CitrixWorkspaceApp.exe /silent`
- Uninstall command: `CitrixWorkspaceApp.exe /uninstall`
- Install behavior: System

g) Click **Requirement**, enter the required information, and then click **OK**.

> **Note:**
>
> Select both x64 and x32 from the Operating System Architecture list. Operating System version can be anything with Win 1607 and later.

h) Click **Detection rules**, select **Manually configure detection rules** as the **Rules format**, and then click **OK**.

i) Click **Add**, select the required **Rule type**, and then click **OK**.

- If **Rule type** is **File** then the path can be, for example, `C:\Program Files (x86)\Citrix\ICA Client\wfica32.exe`.
- If **Rule type** is **Registry**, then enter `HKEY_CURRENT_USER\Software\Citrix` as **Path** and **Key exists** as the **Detection method**.

j) Click **Return codes**, check if the default return codes are valid and then click **OK**.

k) Click **Add** to add the app to Intune.

4. Verify if the deployment is successful:

a) Click **Home** > **Apps** > **Windows**.

b) Click **Device install status**.

Device status displays the number of devices where Citrix Workspace app is installed.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Update

February 27, 2024

Manual update

If you have already installed Citrix Workspace app for Windows, download and install the latest version of the app from the Citrix Downloads page. For information on the installation, see Install and Uninstall.

Automatic update

When a new version of the Citrix Workspace app is available, Citrix pushes the update on the system that has the Citrix Workspace app installed.

> **Note:**
>
> - If you've configured an SSL intercepting outbound proxy, add an exception to the Workspace auto-update server `https://downloadplugins.citrix.com/` to receive updates from Citrix.
> - Auto-update is not available for versions before Citrix Workspace app for Windows 2104 and Citrix Workspace app 1912 LTSR CU4.
> - Your system must have an internet connection to receive updates.
> - By default, Citrix Workspace app updates are disabled on the VDA. It includes RDS multi-user server machines, VDI, and Remote PC Access machines.
> - Citrix Workspace app updates are disabled on machines where Desktop Lock is installed.
> - Workspace for web users can't download the StoreFront policy automatically.
> - Citrix Workspace app updates can be limited to LTSR updates only.
> - Citrix HDX RTME for Windows is included in Citrix Workspace app Updates. A notification appears when updates to the HDX RTME on both LTSR and the current release of the Citrix Workspace app are available.
> - Starting with Version 2105, Citrix Workspace app Updates log paths are modified. The Workspace Updates logs are present at C:\Program Files (x86)\Citrix\Logs. For information on logging, see the Log collection section.
> - A non-administrator can update Citrix Workspace app on an admin-installed instance. You can do that by right-clicking the Citrix Workspace app icon in the notification area and selecting **Check for Updates**. The **Check for Updates** option is available on both the user-installed and the admin-installed instances of Citrix Workspace app.

Restart the Citrix Workspace app for Windows after a manual or automatic update.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

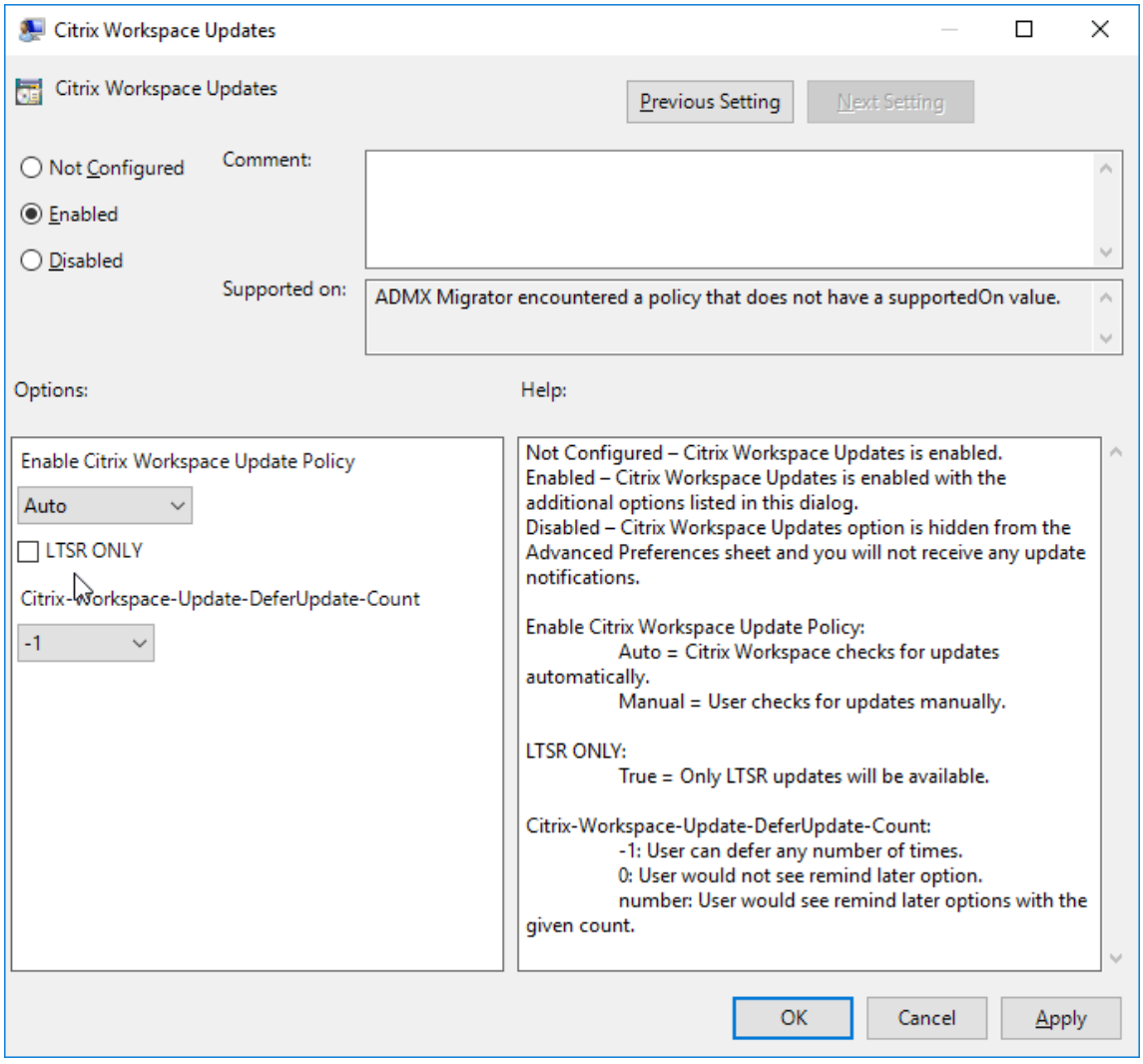
Advanced configuration for automatic updates (Citrix Workspace Updates)

You can configure Citrix Workspace app Updates using the following methods:

1. Group Policy Object (GPO) administrative template
2. Command-line interface
3. GUI
4. StoreFront

Configure Citrix Workspace Updates using the Group Policy Object administrative template

1. Open the Citrix Workspace app Group Policy Object administrative template by running gpedit.msc and navigate to the Computer Configuration node.
2. Go to **Administrative Templates** > **Citrix Components** > **Citrix Workspace** > **Workspace Updates**.



© 1997–2026 Citrix Systems, Inc. All rights reserved.

3. **Enable or disable updates** –Select **Enabled** or **Disabled** to enable or disable Workspace Updates.

   > **Note:**
   >
   > When you select **Disabled**, you aren't notified of new updates. **Disabled** option also hides the Workspace Updates option from the Advanced Preferences sheet.

4. **Update notification** –When an update is available, you can choose to be automatically notified or check for them manually. After you have enabled Workspace updates, select one of the following options from the **Enable Citrix Workspace app Update Policy** drop-down list:

   - Auto - You're notified when an update is available (default).
   - Manual - You aren't notified when an update is available. Check for updates manually.

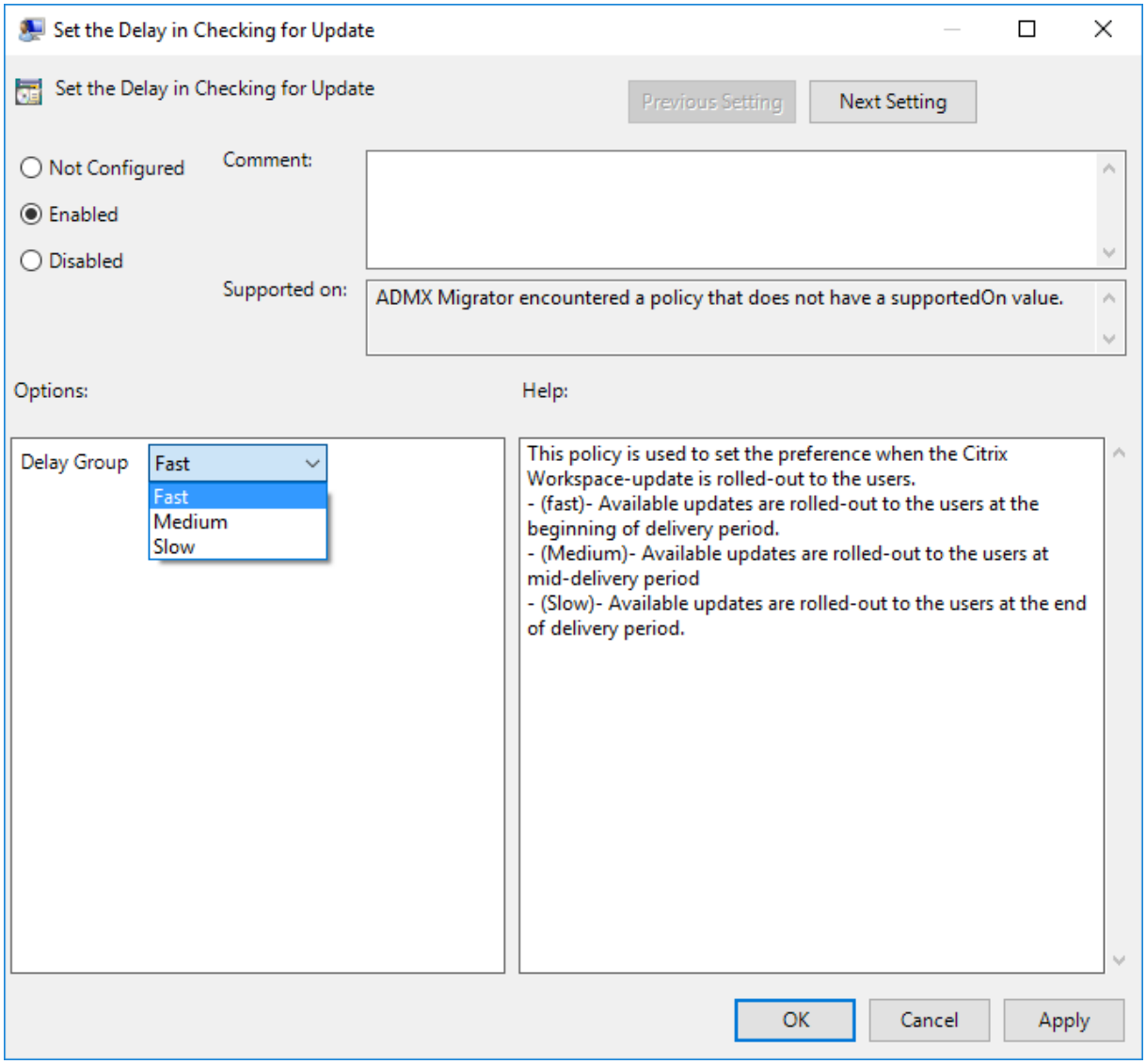
5. Select **LTSR ONLY** to get updates for LTSR only.
6. From the **Citrix-Workspace-Update-DeferUpdate-Count** drop-down list, select a value between -1 and 30:

   - If the value is 0 then the **Remind Me Later** option appears. **Update available** prompt is shown on every periodic automatic check for update.
   - If the value is -1 then the **Remind Me Later** option appears with the **Update available** prompt. You can defer the update notification any number of times.
   - A value between 1-30 defines the number of times the **Remind Me Later** option with the **Update available** prompt must appear. You can defer the update notification based on the value defined in this field. However, the **Update available** prompt continues to appear but without the **Remind Me Later** option.

Configure the delay in checking for updates When a new version of the Citrix Workspace app is available, Citrix rolls out the update during a specific delivery period. With this property, you can control at what stage during the delivery period you can receive the update.

To configure the delivery period, run `gpedit.msc` to launch the Group Policy Object administrative template. Under **Computer Configuration** node, go to **Administrative Templates** > **Citrix Components** > **Citrix Workspace** > **Set the Delay in Checking for Update**.

© 1997–2026 Citrix Systems, Inc. All rights reserved.



Select **Enabled**, and from the **Delay Group** drop-down list, select one of the following:

- Fast –Update rollout happens at the beginning of the delivery period.
- Medium –Update rollout happens at the mid-delivery period.
- Slow –Update rollout happens at the end of the delivery period.

> **Note:**
>
> When you select **Disabled**, you aren't notified of available updates. **Disabled** also hides the Workspace Updates option from the Advanced Preferences sheet.

Configure Citrix Workspace app Updates using the command-line interface

By specifying command-line parameters while installing Citrix Workspace app:

© 1997–2026 Citrix Systems, Inc. All rights reserved.

You can configure Workspace updates by specifying command-line parameters during the Citrix Workspace app installation. See Install parameters for more information.

By using command-line parameters after Citrix Workspace app has been installed:

Citrix Workspace Updates can also be configured after installing the Citrix Workspace app for Windows. Navigate to the location of `CitrixReceiverUpdater.exe` using the Windows command line.

Typically, CitrixReceiverUpdater.exe is at `CitrixWorkspaceInstallLocation\Citrix\Ica Client\Receiver`. You might run the `CitrixReceiverUpdater.exe` binary along with the command-line parameters listed in the Install parameters section.

For example,

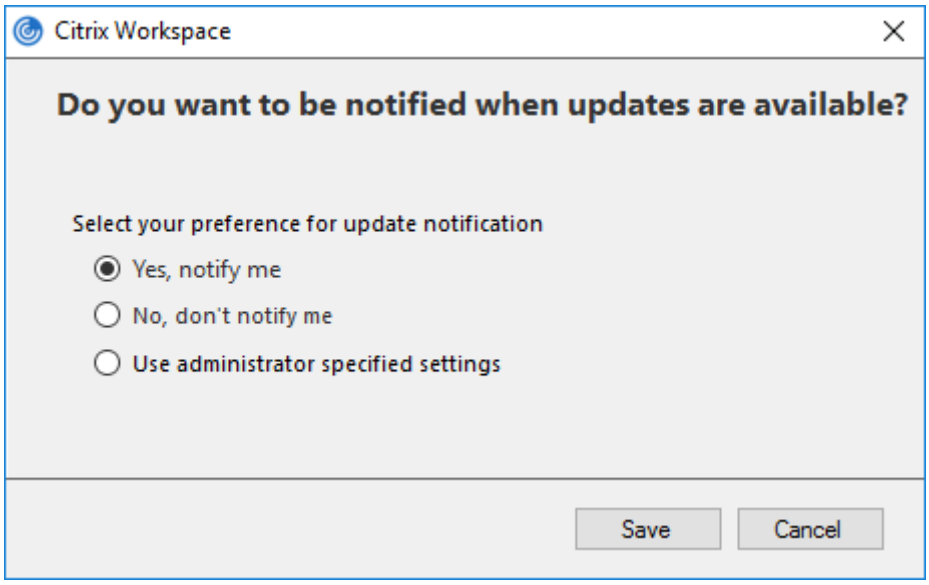
```
CitrixReceiverUpdater.exe /AutoUpdateCheck=auto /AutoUpdateStream=
Current /DeferUpdateCount=-1 /AURolloutPriority=fast
```

> **Note**:
>
> The `/AutoUpdateCheck` is a mandatory parameter that you must set to configure other parameters like `/AutoUpdateStream`, `/DeferUpdateCount`, `/AURolloutPriority`.

Configure Citrix Workspace Updates using the graphical user interface

Individual user can override the **Citrix Workspace Updates** setting using the **Advanced Preferences** dialog. This is a per-user configuration and the settings apply only to the current user.

1. Right-click Citrix Workspace app icon from the notification area.
2. Select **Advanced Preferences** > **Citrix Workspace Updates**.
3. Select the notification preference and click **Save**.



© 1997–2026 Citrix Systems, Inc. All rights reserved.

> **Note:**
>
> You can hide all or part of the Advanced Preferences sheet available from the Citrix Workspace app icon. For more information, see the Advanced Preferences sheet section.

Configure Citrix Workspace app Updates using StoreFront

1. Use a text editor to open the `web.config` file, which is typically at `C:\inetpub\wwwroot\Citrix\Roaming directory`.
2. Locate the user account element in the file (Store is the account name of your deployment)

   For example: `<account id=... name="Store">`

   Before the `</account>` tag, navigate to the properties of that user account:

```
<properties>
       <clear/>
 </properties>
```

3. Add the auto-update tag after the *<clear />* tag.

```
<account>

    <clear />

    <account id="d1197d2c-ac82-4f13-9346-2ee14d4b0202" name="
       F84Store"

      description="" published="true" updaterType="Citrix"
         remoteAccessType="None">

      <annotatedServices>

        <clear />

        <annotatedServiceRecord serviceRef="1__Citrix_F84Store">

          <metadata>

            <plugins>

              <clear />

            </plugins>

            <trustSettings>

              <clear />

            </trustSettings>
```

© 1997–2026 Citrix Systems, Inc. All rights reserved.

```
28
29              <properties>
30
31                <property name="Auto-Update-Check" value="auto" />
32
33                <property name="Auto-Update-DeferUpdate-Count" value
                     ="1" />
34
35                       <property name="Auto-Update-LTSR-Only" value
                          ="FALSE" />
36
37                <property name="Auto-Update-Rollout-Priority" value=
                     "fast" />
38
39                    </properties>
40
41            </metadata>
42
43          </annotatedServiceRecord>
44
45        </annotatedServices>
46
47        <metadata>
48
49          <plugins>
50
51            <clear />
52
53          </plugins>
54
55          <trustSettings>
56
57            <clear />
58
59          </trustSettings>
60
61          <properties>
62
63            <clear />
64
65          </properties>
66
67        </metadata>
68
69      </account>
```

The meaning of the properties and their possible values are detailed as follows:

- **Auto-update-Check:** Indicates that Citrix Workspace app detects an update automatically when available.
- **Auto-update-LTSR-Only:** Indicates that the update is for LTSR only.
- **Auto-update-Rollout-Priority:** Indicates the delivery period in which you can receive the up-

© 1997–2026 Citrix Systems, Inc. All rights reserved.

date.

- **Auto-update-DeferUpdate-Count:** Indicates the number of counts that you can defer the notifications for the updates.

Get started

July 17, 2026

This article is a reference document to help you set up your environment after you install Citrix Workspace app.

Prerequisites:

Verify that all the requirements are met as listed in the System requirements section.

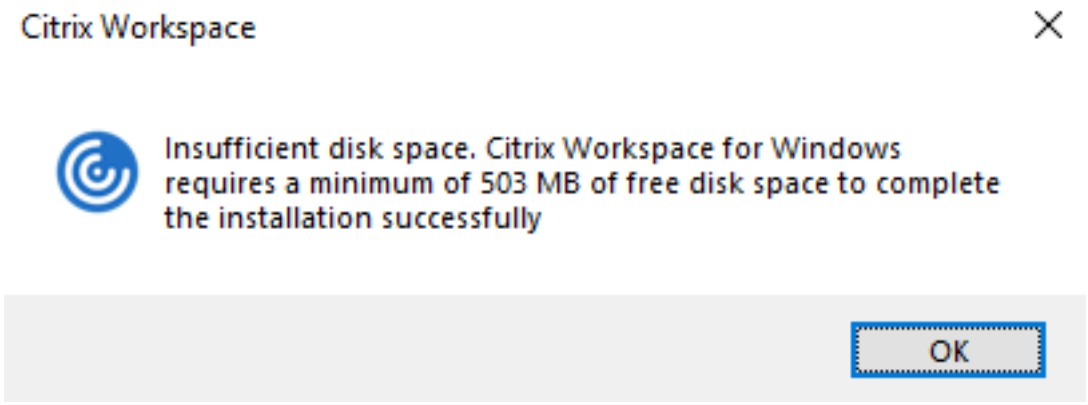
Validating free disk space

See the following table for details on disk space required before installation:

Installation type	Minimum disk space required
Fresh installation	572 MB
Upgrade	350 MB

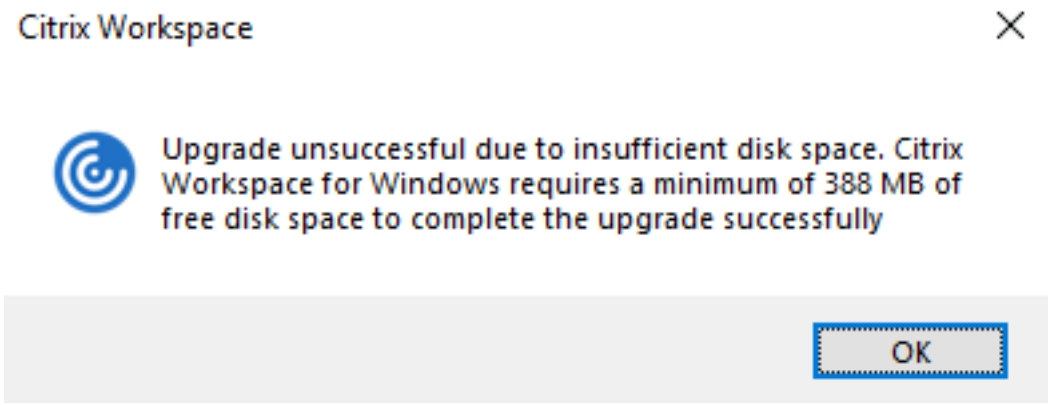
Citrix Workspace app does a check to verify available disk space to complete the installation. The verification is done both during a fresh installation and an upgrade.

During a fresh installation, the installation stops and the following dialog appears when there's insufficient disk space:



© 1997–2026 Citrix Systems, Inc. All rights reserved.

When you're upgrading Citrix Workspace app, the installation ends and the following dialog box appears when there's insufficient disk space.



Note:

- The installer checks the disk space only after extracting the installation package.
- When the system is low on disk space during silent installation, the dialog does not appear but the error message is recorded in the `CTXInstall\\_TrolleyExpress-\*.log`.

Configure the following before using the Citrix Workspace app:

- StoreFront
- Citrix Gateway Store
- Adding store URL to Citrix Workspace app
- Client drive mapping
- Domain Name Service name resolution

Group Policy Object administrative template

We recommend that you use the Group Policy Object administrative template to configure rules for:

- Network routing
- Proxy servers
- Trusted server configuration
- User routing
- Remote user devices
- User experience.

You can use the `receiver.admx` / `receiver.adml` template files with domain policies and local computer policies. For domain policies, import the template file using the Group Policy Management console. Importing is useful when applying Citrix Workspace app settings to several different user

© 1997–2026 Citrix Systems, Inc. All rights reserved.

devices throughout the enterprise. To modify on a single user device, import the template file using the local Group Policy Editor on the device.

Citrix recommends using the Windows Group Policy Object (GPO) administrative template to configure Citrix Workspace app.

The installation directory includes `CitrixBase.admx` and `CitrixBase.adml`, and, administrative template files (`receiver.adml` or `receiver.admx`'receiver.adml').

> **Note:**
>
> The .admx and .adml files are for use with Windows Vista, Windows Server 2008, and other later versions of Windows.

For example: `\<installation directory\>\Online Plugin\Configuration`.

If Citrix Workspace app is installed without the VDA, the admx/adml files are typically found in the `C:\Program Files\Citrix\ICA Client\Configuration` directory.

See the following table for information about Citrix Workspace app template files and their respective locations.

> **Note:**
>
> Citrix recommends that you use the GPO template files provided with latest version of Citrix Workspace app.

File type	File location
receiver.adm	\ICA Client\Configuration
receiver.admx	\ICA Client\Configuration
receiver.adml	\ICA Client\Configuration\[MUIculture]
CitrixBase.admx	\ICA Client\Configuration
CitrixBase.adml	\ICA Client\Configuration\[MUIculture]

> **Note:**
>
> - If the CitrixBase.admx\adml isn't added to the local GPO, the **Enable ICA File Signing** policy might be lost.
> - When upgrading Citrix Workspace app, add the latest template files to local GPO. Earlier settings are retained after import. For more information, see the following procedure:

© 1997–2026 Citrix Systems, Inc. All rights reserved.

To add the receiver.admx/adml template files to the local GPO:

You can use .adm template files to configure both the Local and the domain-based GPO. Refer to the Microsoft MSDN article about managing ADMX files here.

After installing Citrix Workspace app, copy the following template files:

File type	Copy from	Copy to
receiver.admx	`Installation Directory\ICA Client\Configuration\receiver.admx`	`%systemroot%\policyDefinitions`
CitrixBase.admx	`Installation Directory\ICA Client\Configuration\CitrixBase.admx`	`%systemroot%\policyDefinitions`
receiver.adml	`Installation Directory\ICA Client\Configuration\[MUIculture]receiver.adml`	`%systemroot%\policyDefinitions\[MUIculture]`
CitrixBase.adml	`Installation Directory\ICA Client\Configuration\[MUIculture]\CitrixBase.adml`	`%systemroot%\policyDefinitions\[MUIculture]`

> **Note:**
>
> Add the CitrixBase.admx/CitrixBase.adml to the `\PolicyDefinitions` folder to view the template files in **Administrative Templates** > **Citrix Components** > **Citrix Workspace**.

StoreFront

Configure Citrix Gateway to enable users to connect from outside the internal network. For example, users who connect from the Internet or from remote locations.

> **Note:**
>
> You might see the old StoreFront user interface if you select The **Show all Stores** option.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

To configure StoreFront:

Install and configure StoreFront as described in the StoreFront documentation. Citrix Workspace app requires an HTTPS connection. On an HTTP configured StoreFront, set the registry key as described in Using command-line parameters.

> **Note:**
>
> Citrix provides a template you can use to create a download site for Citrix Workspace app for Windows.

Citrix Gateway Store

To add or specify a Citrix Gateway using the Group Policy Object administrative template:

1. Open the Citrix Workspace app Group Policy Object administrative template by running gpedit.msc.
2. Under the **Computer Configuration node**, go to **Administrative Templates** > **Classic Administrative Templates (ADM)** > **Citrix Components** > **Citrix Workspace** > **StoreFront**.
3. Select **Citrix Gateway URL/StoreFront Accounts List**.
4. Edit the settings.
    - Store name –Indicates the displayed store name
    - Store URL –Indicates the URL of the store
    - #Store name –Indicates the name of the store behind Citrix Gateway
    - Store enabled state –Indicates the state of the store, On or Off
    - Store Description –Provides description of the store
5. Add or specify the Citrix Gateway URL. Enter the name of the URL, delimited by a semi-colon:

Example: `CitrixWorkspaceApp.exe STORE0= HRStore;https://ag.mycompany.com#Storename;On;Store`
Where #Store name is the name of the store behind Citrix Gateway.

Starting with Version 1808, changes made to the **Citrix Gateway URL/StoreFront Account List** policy are applied in a session after app restart. A reset isn't required.

> **Note:**
>
> Citrix Workspace app Version 1808 and later doesn't require resetting on a fresh installation. If there's an upgrade to 1808 or later, you must reset the Citrix Workspace app for the changes to take effect.

Limitations:

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- Citrix Gateway URL must be listed as first followed by StoreFront URLs.
- No support for Multiple Citrix Gateway URLs.
- Citrix Gateway URL configured using this method does not support the PNA Services site behind Citrix Gateway.

Manage workspace control reconnect

Workspace control lets applications follow users as they move between devices. For example, workspace control enables clinicians in hospitals to move from workstation to workstation without having to restart their applications on each device. For Citrix Workspace app, you manage workspace control on client devices by modifying the registry. Workspace control can also be done for domain-joined client devices using Group Policy.

> **Caution**
>
> Editing the registry incorrectly can cause serious problems that might require you to reinstall your operating system. Citrix can't guarantee that problems resulting from the incorrect use of the Registry Editor can be solved. Use the Registry Editor at your own risk. Be sure to back up the registry before you edit it.

Create **WSCReconnectModeUser** and modify the existing registry key **WSCReconnectMode** in the Master Desktop Image or in the Citrix Virtual Apps server. The published desktop can change the behavior of the Citrix Workspace app.

WSCReconnectMode key settings for Citrix Workspace app:

- 0 = do not reconnect to any existing sessions
- 1 = reconnect on application launch
- 2 = reconnect on application refresh
- 3 = reconnect on application launch or refresh
- 4 = reconnect when Citrix Workspace interface opens
- 8 = reconnect on Windows sign-on
- 11 = combination of both 3 and 8

Disable workspace control To disable workspace control, create the following key:

`HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Citrix\Dazzle` (64-bit)

`HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\\Dazzle` (32-bit)

Name: **WSCReconnectModeUser**

Type: REG_SZ

Value data: `0`

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Modify the following key from the default value of 3 to zero

`HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Citrix\Dazzle` (64-bit)

`HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\Dazzle` (32-bit)

Name: **WSCReconnectMode**

Type: REG_SZ

Value data: `0`

> **Note:**
>
> You can also set the **WSCReconnectAll** key to false if you don't want to create a key.

Changing the status indicator timeout

You can change the amount of time the status indicator displays when a user is launching a session. To alter the time-out period, create a REG_DWORD value `SI INACTIVE MS` in `HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\ICA CLIENT\Engine\`. The REG_DWORD value can be set to 4 if you want the status indicator to disappear sooner.

Customizing location for application shortcut using command line

The start menu integration and desktop shortcut only feature lets you bring published application shortcuts into the **Windows Start** menu and onto the desktop. Users do not have to subscribe to applications from the Citrix Workspace user interface. Start menu integration and desktop shortcut management provide a seamless desktop experience for groups of users. Also for users who need access to a core set of applications in a consistent way.

The flag is called **SelfServiceMode** and is set to `True` by default. When the administrator sets the **SelfServiceMode** flag to `False`, you can't access the self-service user interface. Instead, you can access subscribed apps from the Start menu and desktop shortcuts that is referred as shortcut-only mode.

Users and administrators can use several registry settings to customize the way shortcuts are set up.

Working with shortcuts

- Users can't remove apps. All apps are mandatory when working with the **SelfServiceMode** flag set to false (shortcut-only mode). If you remove a shortcut icon from the desktop, the icon comes back when the user selects **Refresh** from the Citrix Workspace app icon in the notification area.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- Users can configure only one store. The Account and Preferences options aren't available to prevent the user from configuring more stores. The administrator can give a user special privileges to add more than one account using the Group Policy Object template. Administrators can also provide special privileges by manually adding a registry key (HideEditStoresDialog) on the client machine. When the administrator gives a user this privilege, the user has a Preferences option in the notification area, where they can add and remove accounts.
- Users can't remove apps using the **Windows Control** Panel.
- You can add desktop shortcuts via a customizable registry setting. Desktop shortcuts aren't added by default. After editing the registry settings, restart the Citrix Workspace app.
- Shortcuts are created in the Start menu with a category path as the default, UseCategoryAsStartMenuPath.

> **Note:**
>
> Windows 8/8.1 and Windows 10 do not allow the creation of nested folders within the Start menu. Applications are displayed individually or under the root folder. But, not within the Category sub folders that are defined with Citrix Virtual Apps.

- You can add a flag [/DESKTOPDIR="Dir_name"] during installation to bring all shortcuts into a single folder. CategoryPath is supported for desktop shortcuts.
- Auto Reinstall Modified Apps feature can be enabled using the registry key `AutoReInstallModifiedApp`. When `AutoReInstallModifiedApps` is enabled, any changes to the published apps and desktops attributes on the server are displayed on the client machine. When `AutoReInstallModifiedApps` is disabled, apps and desktop attributes aren't updated and shortcuts aren't restored on refresh if deleted on the client. By default, the `AutoReInstallModifiedApps` is enabled.

Customizing location for application shortcut using the Registry editor

> **Note:**
>
> - By default, registry keys use the **String** format.
> - Change registry keys before you configure a store. If at any time you or a user wants to customize the registry keys, you or the user must:
>
> 1. reset Citrix Workspace app
> 2. configure the registry keys, and then
> 3. reconfigure the store.

Registry keys for 32-bit machines

Registry key: WSCSupported **Value**: `True`

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Key path:

```
- HKEY_CURRENT_USER\Software\Citrix\Dazzle
- HKEY_CURRENT_USER\Software\Citrix\Receiver\SR\Store" +
  primaryStoreID +\Properties
- HKEY_LOCAL_MACHINE\Software\Policies\Citrix\Dazzle
- HKEY_LOCAL_MACHINE\Software\Citrix\Dazzle
```

Registry key: WSCReconnectAll **Value**: `True`

Key path:

```
- `HKEY_CURRENT_USER\Software\Citrix\Dazzle`
- `HKEY_CURRENT_USER\Software\Citrix\Receiver\SR\Store" +
  primaryStoreID + \Properties`
- `HKEY_LOCAL_MACHINE\Software\Policies\Citrix\Dazzle`
- `HKEY_LOCAL_MACHINe\Software\Citrix\Dazzle`
```

Registry key: WSCReconnectMode **Value**: 3

Key path:

```
- HKEY_CURRENT_USER\Software\Citrix\Dazzle
- HKEY_CURRENT_USER\Software\Citrix\Receiver\SR\Store" +
  primaryStoreID +\Properties
- HKEY_LOCAL_MACHINE\Software\Policies\Citrix\Dazzle
- HKEY_LOCAL_MACHINE\Software\Citrix\Dazzle
```

Registry key: WSCReconnectModeUser **Value**: Registry isn't created during installation.

Key path:

```
- HKEY_CURRENT_USER\Software\Citrix\Dazzle
- HKEY_CURRENT_USER\Software\Citrix\Receiver\SR\Store" + primaryStoreID
  +\Properties
- HKEY_LOCAL_MACHINE\Software\Policies\Citrix\Dazzle
- HKEY_LOCAL_MACHINE\Software\Citrix\Dazzle
```

Registry keys for 64-bit machines:

Registry key: WSCSupported **Value**: `True`

Key path:

```
- HKEY_CURRENT_USER\Software\Citrix\Dazzle
- HKEY_CURRENT_USER\Software\Citrix\Receiver\SR\Store" + primaryStoreID
  +\Properties
- HKEY_LOCAL_MACHINE\Software\Wow6432Node\Policies\Citrix\Dazzle
- HKEY_LOCAL_MACHINE\Software\Wow6432Node\Citrix\Dazzle
```

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Registry key: WSCReconnectAll **Value**: True

Key path:

```
- HKEY_CURRENT_USER\Software\Citrix\Dazzle
- HKEY_CURRENT_USER\Software\Citrix\Receiver\SR\Store" +
  primaryStoreID + \Properties
- HKEY_LOCAL_MACHINE\Software\Wow6432Node\Policies\Citrix\Dazzle
- HKEY_LOCAL_MACHINE\Software\Wow6432Node\Citrix\Dazzle
```

Registry key: WSCReconnectMode **Value**: 3

Key path:

```
- HKEY_CURRENT_USER\Software\Citrix\Dazzle
- HKEY_CURRENT_USER\Software\Citrix\Receiver\SR\Store" +
  primaryStoreID +\Properties
- HKEY_LOCAL_MACHINE\Software\Wow6432Node\Policies\Citrix\Dazzle
- HKEY_LOCAL_MACHINE\Software\Wow6432Node\Citrix\Dazzle
```

Registry key: WSCReconnectModeUser **Value**: Registry isn't created during installation.

Key path:

```
- HKEY_CURRENT_USER\Software\Citrix\Dazzle
- HKEY_CURRENT_USER\Software\Citrix\Receiver\SR\Store" + primaryStoreID
   +\Properties
- HKEY_LOCAL_MACHINE\Software\Wow6432Node\Policies\Citrix\Dazzle
- HKEY_LOCAL_MACHINE\Software\Wow6432Node\Citrix\Dazzle
```

User accounts

You can provide users with the account information that they need to access virtual desktops and application using the following:

- Configuring email-based account discovery
- Provisioning file
- Providing users with account information to enter manually

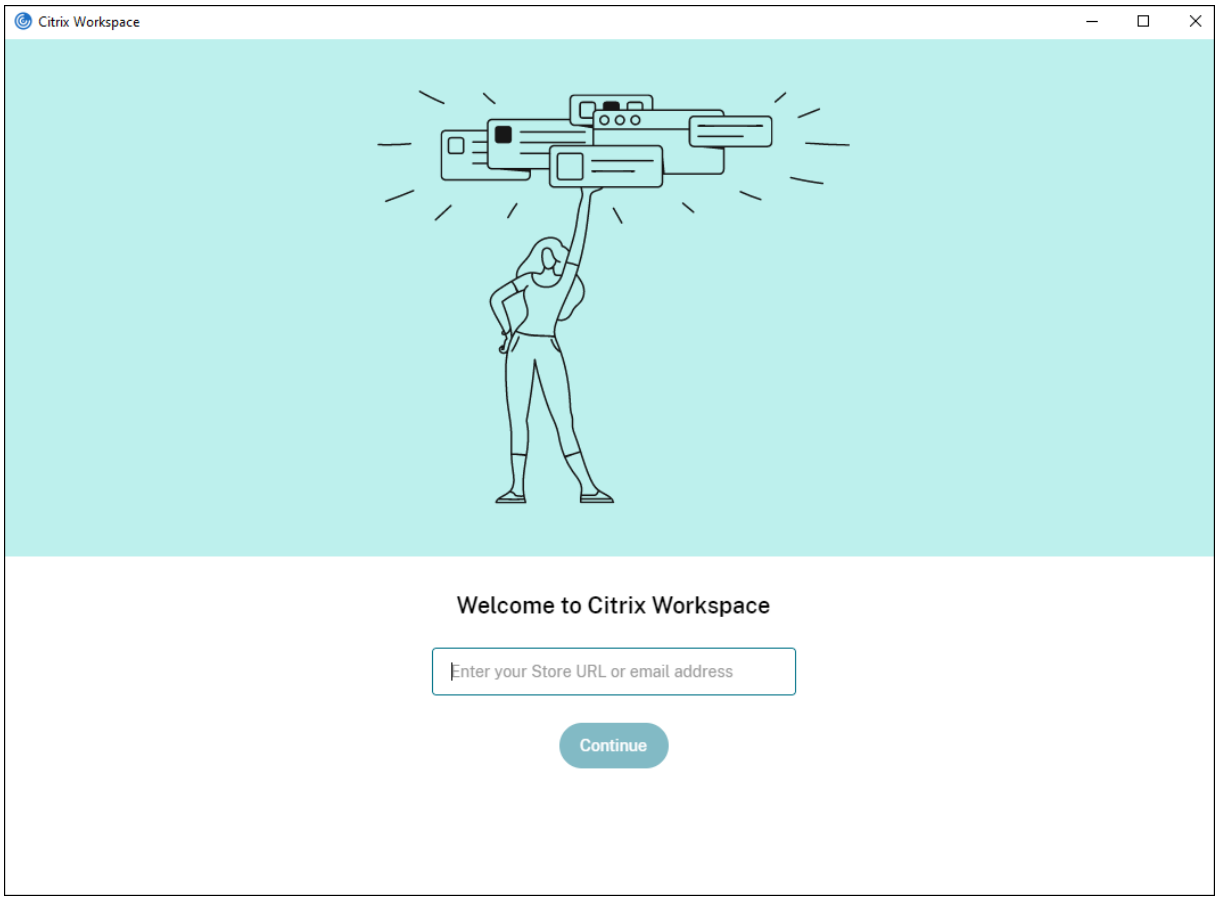
> **Important**
>
> Citrix recommends that you restart Citrix Workspace app after the installation to ensure that:
>
> - Restart ensures that users can add accounts and
> - Citrix Workspace app can discover USB devices that were in a suspended state during installation.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

A dialog appears to indicate a successful installation, followed by the **Add Account** dialog. For a first time user, the **Add Account** dialog requires you to enter an email or server address to set up an account.

Provide users with account information to enter manually

Upon successful installation of Citrix Workspace app, the following screen appears. Users are required to enter an email or server address to access the apps and desktops. When a user enters the details for a new account, Citrix Workspace app tries to verify the connection. If successful, Citrix Workspace app prompts the user to log on to the account.



To enable users to set up accounts manually, be sure to distribute the information they need to connect to their virtual desktops and applications.

- To connect to a cloud store, provide the cloud store URL.
- To connect to a StoreFront store, provide the URL for that server. For example:`https://servername.company.com`.
- To connect through Citrix Gateway, first determine whether a user must see all configured stores or just the store with remote access enabled for a particular Citrix Gateway.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- To present all configured stores: Provide users with the Citrix Gateway fully qualified domain name.
- To limit access to a particular store: Provide users with the Citrix Gateway fully qualified domain name and the store name in the form:

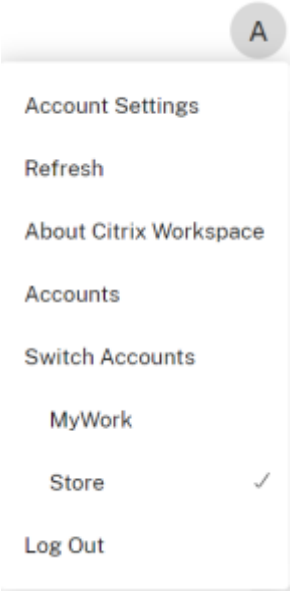
  CitrixGatewayFQDN?MyStoreName:

  For example, if a store named "SalesApps"has remote access enabled for server1.com and a store named **HRApps** has remote access enabled for server2.com, a user must enter:

  - server1.com?SalesApps to access SalesApps or
  - server2.com?HRApps to access **HRApps**.

  CitrixGatewayFQDN?MyStoreName feature requires a new user to create an account by entering a URL and isn't available for email-based discovery.

Once the Citrix Workspace app is configured with the Store URL, the account can be managed from the **Accounts** option in the profile menu.



Configure email-based account discovery

When you configure Citrix Workspace app for email-based account discovery, users enter their email address rather than a server URL during initial Citrix Workspace app installation and configuration. Citrix Workspace app determines the Citrix Gateway or StoreFront Server associated with the email address based on Domain Name System (DNS) Service (SRV) records. The app then prompts the user to log on to access virtual desktops and applications.

For more information, see Configuring email based account discovery.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Provide users with provisioning files

StoreFront provides provisioning files that users can open to connect to stores.

You can use StoreFront to create provisioning files that include connection details for accounts. Make these files available to your users to enable them to configure Citrix Workspace app automatically. After installing Citrix Workspace app, users simply open the file to configure Citrix Workspace app. If you configure workspace for web, users can also get Citrix Workspace app provisioning files from those sites.

For more information, see To export store provisioning files for users in the StoreFront documentation.

Provide users with account information to enter manually

To enable users to set up accounts manually, be sure to distribute the information they need to connect to their virtual desktops and applications.

- To connect to a StoreFront store, provide the URL for that server. For example:`https://servername.company.com`.
- To connect through Citrix Gateway, first determine whether a user must see all configured stores or just the store with remote access enabled for a particular Citrix Gateway.
    - To present all configured stores: Provide users with the Citrix Gateway fully qualified domain name.
    - To limit access to a particular store: Provide users with the Citrix Gateway fully qualified domain name and the store name in the form:

CitrixGatewayFQDN?MyStoreName:

For example, if a store named "SalesApps"has remote access enabled for server1.com and a store named **HRApps** has remote access enabled for server2.com, a user must enter:

- server1.com?SalesApps to access SalesApps or
- server2.com?HRApps to access **HRApps**.

CitrixGatewayFQDN?MyStoreName feature requires a new user to create an account by entering a URL and isn't available for email-based discovery.

When a user enters the details for a new account, Citrix Workspace app tries to verify the connection. If successful, Citrix Workspace app prompts the user to log on to the account.

To manage accounts, open the Citrix Workspace app home page, and click , and then click **Accounts**.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Sharing multiple stores accounts automatically

> **Warning**
>
> Using the Registry Editor incorrectly can cause serious problems that require you to reinstall the operating system. Citrix can't guarantee that problems resulting from incorrect use of the Registry Editor can be solved. Use the Registry Editor at your own risk. Back up the registry before you edit it.

If you've more than one store account, you can configure Citrix Workspace app for Windows to automatically connect to all accounts when establishing a session. To automatically view all accounts when opening Citrix Workspace app:

For 32-bit systems:

Key path: `HKEY_LOCAL_MACHINE\Software\Citrix\Dazzle`

KeyName: `CurrentAccount`

Value: `AllAccount`

Type: REG_SZ

For 64-bit systems:

Key path: `HKEY_LOCAL_MACHINE\\Software\\Wow6432Node\\Citrix\\Dazzle`

KeyName: CurrentAccount

Value: AllAccount

Type: REG_SZ

Client drive-mapping

Citrix Workspace app for Windows supports device mapping on user devices so they're available from within a session. Users can:

- Transparently access local drives, printers, and COM ports
- Cut and paste between the session and the local Windows clipboard
- Hear audio (system sounds and .wav files) played from the session

Citrix Workspace app informs the server of the available client drives, COM ports, and LPT ports during sign-in. By default, client drives are mapped to server drive letters and server print queues are created for client printers, which make them appear to be directly connected to the session. These mappings are available only for the current user during the current session. They're deleted when the user logs off and recreated the next time the user logs on.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

You can use the redirection policy settings to map user devices not automatically mapped at logon. For more information, see the Citrix Virtual Apps and Desktops™ documentation.

Disable user device mappings

You can configure user device-mapping including options for drives, printers, and ports, using the **Windows Server Manager** tool. For more information about the available options, see your Remote Desktop Services documentation.

Redirect client folders

Client folder redirection changes the way client-side files are accessible on the host-side session. Enabling only client drive mapping on the server, client-side full volumes automatically maps to the sessions as Universal Naming Convention (UNC) links. When you enable client folder redirection on the server and the user configures it on the user device, part of the user specified local volume gets redirected.

Only the user-specified folders appear as UNC links inside the sessions, instead of the complete file system on the user device. If you disable UNC links through the registry, client folders appear as mapped drives inside the session. For more information, including how to configure client folder redirection for user devices, see the Citrix Virtual Apps and Desktops documentation.

Map client drives to host-side drive letters

Client drive mapping redirects drive letters on the host-side to drives that exist on the user device. For example, drive H in a Citrix user session can be mapped to drive C of the user device running Citrix Workspace app for Windows.

Client drive mapping is built into the standard Citrix device redirection facilities transparently. To File Manager, Windows Explorer, and your applications, these mappings appear like any other network mappings.

The server hosting virtual desktops and applications can be configured during installation to map client drives automatically to a given set of drive letters. The default installation maps drive letters assigned to client drives starting with V and works backward, assigning a drive letter to each fixed drive and CD-ROM drive. (Floppy drives are assigned their existing drive letters.) This method yields the following drive mappings in a session:

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Client drive letter	Accessible by the server as
A	A
B	B
C	V
D	U

The server can be configured so that the server drive letters don't conflict with the client drive letters. So, the server drive letters are changed to higher drive letters.
In the following example, changing server drives C to M and D to N allows client devices to access their C and D drives directly. This method yields the following drive mappings in a session:

Client drive letter	Accessible by the server as
A	A
B	B
C	C
D	D

The drive letter used to replace the server drive C is defined during Setup. All other fixed drive and CD-ROM drive letters are replaced with sequential drive letters (for example; C > M, D > N, E > O). These drive letters must not conflict with any existing network drive mappings. If you map the network drive to the same drive letter as a server drive letter, the network drive mapping isn't valid.

Connecting a user device to a server, reestablishes client mappings unless automatic client device mapping is disabled. Client drive mapping is enabled by default. To change the settings, use the Remote Desktop Services (Terminal Services) Configuration tool. You can also use policies to give you more control over how client device mapping is applied. For more information about policies, see the Citrix Virtual Apps and Desktops documentation.

HDX™ Plug and Play USB device redirection

HDX Plug and Play USB device redirection enables dynamic redirection of media devices to the server. The media device includes cameras, scanners, media players, and point of sale (POS) devices. You or the user can restrict the redirection of all or some of the devices. Edit policies on the server or apply group policies on the user device to configure the redirection settings. For more information, see USB and client drive considerations in the Citrix Virtual Apps and Desktops documentation.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

> **Important**
>
> If you prohibit Plug and Play USB device redirection in a server policy, the user can't override that policy setting.

A user can set permissions in Citrix Workspace app to allow or reject device redirection always or notify each time a device is connected. The setting affects only devices plugged in after the user changes the setting.

To map a client COM port to a server COM port:

Client COM port mapping allows devices attached to the COM ports of the user device to be used during sessions. These mappings can be used like any other network mappings.

You can map client COM ports at the command prompt. You can also control client COM port mapping from the Remote Desktop (Terminal Services) Configuration tool or using policies. For information about policies, see the Citrix Virtual Apps and Desktops documentation.

> **Important**
>
> COM port mapping isn't TAPI-compatible.

1. For Citrix Virtual Apps and Desktops deployments, enable the Client COM port redirection policy setting.
2. Log on to Citrix Workspace app.
3. At a command prompt, type:

   ```
   net use comx: \\\\\client\\comz:
   ```

   where:

   - x is the number of the COM port on the server (ports 1 through 9 are available for mapping) and
   - z is the number of the client COM port you want to map

4. To confirm the operation, type:

   ```
   net use
   ```

   The prompt displays mapped drives, LPT ports, and mapped COM ports.

To use this COM port in a virtual desktop or application, install your user device to the mapped name. For example, if you map COM1 on the client to COM5 on the server, install your COM port device on COM5 during the session. Use this mapped COM port as you would a COM port on the user device.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Domain Name Service name resolution

You can configure Citrix Workspace app for Windows that uses the Citrix XML Service to request a Domain Name Service (DNS) name for a server instead of an IP address.

> **Important:**
>
> Unless your DNS environment is configured specifically to use this feature, Citrix recommends that you do not enable DNS name resolution on the server.

By default, DNS name resolution is disabled on the server and enabled on the Citrix Workspace app. When DNS name resolution is disabled on the server, any Citrix Workspace app request for a DNS name returns an IP address. There's no need to disable DNS name resolution on Citrix Workspace app.

To disable DNS name resolution for specific user devices:

If your server deployment uses DNS name resolution and you experience issues with specific user devices, you can disable DNS name resolution for those devices.

> **Caution**
>
> Using the Registry Editor incorrectly might cause serious problems that require you to reinstall the operating system. We do not guarantee that problems resulting from incorrect use of the Registry Editor can be solved. Use the Registry Editor at your own risk. Back up of the registry before you edit it.

1. Add a string registry key **xmlAddressResolutionType** to `HKEY\\_LOCAL\\_MACHINE\Software\Wow6432Node\Citrix\ICA Client\Engine\Lockdown Profiles\All Regions\Lockdown\Application Browsing`.
2. Set the value to **IPv4-Port**.
3. Repeat for each user of the user devices.

Custom web stores

This feature provides access to your organization's custom web store from the Citrix Workspace app for Windows. To use this feature, the admin must add the domain or custom web store to the Global App Configuration Service allowed URLs.

For more information about configuring web store URLs for end-users, see Global App Configuration Service.

You can now provide the custom web store URL in the **Add Account** screen in Citrix Workspace app. The custom web store opens in the native Citrix Workspace app window.

To remove the custom web store, go to **Accounts** > **Add or Remove accounts**, select the custom web store URL, and click **Remove**.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Configure

July 17, 2026

When using the Citrix Workspace app for Windows, the following configurations allow you to access their hosted applications and desktops.

Microsoft Teams

- Screen sharing
- Encoder performance estimator
- Acoustic Echo Cancellation

Screen sharing

Starting with Version 2006.1, new functionalities in the outgoing screen sharing feature for the Microsoft Teams application that uses HDX optimization are introduced.

The contents shared using Microsoft Teams are limited to the contents of the **Desktop Viewer** window. Areas outside the **Desktop Viewer** window (client local desktop, apps) are blacked out.

On a Windows 10 operating system, the following aren't blacked out when they overlap the **Desktop Viewer** window:

- Start menu, Search menu, and Task View.
- Notification bar and Notifications that appear at the right-side of the task bar.
- On a multi-monitor set up with different DPI settings. If a local app is overlapping 2 different monitors and its DPI doesn't match the main monitor DPI which has the Desktop Viewer window.
- App and preview shown when you mouse-hover over the app's icon in the task bar.

Encoder performance estimator

The `HdxRtcEngine.exe` is the WebRTC media engine embedded in Citrix Workspace app that handles Microsoft Teams redirection. Starting from Citrix Workspace app 1912 or higher, `HdxRtcEngine.exe` can estimate the best encoding resolution that the endpoint's CPU can sustain without overloading. The possible values are 240p, 360p, 480p, 720p, and 1080p.

The performance estimation process (also called `webrtcapi.EndpointPerformance`) runs when HdxTeams.exe initializes. The macroblock code determines the best resolution that can be

© 1997–2026 Citrix Systems, Inc. All rights reserved.

achieved with the particular endpoint. The Codec negotiation includes the highest possible resolution. The Codec negotiation can be between the peers, or between the peer and the conference server.

There are four performance categories for endpoints that have its own **maximum** available resolution:

Endpoint performance	Maximum resolution	Registry key value
fast	1080p (1920x1080 16:9 @ 30 fps)	3
medium	720p (1280x720 16:9 @ 30 fps)	2
slow	360p (either 640x360 16:9 @ 30 fps, or 640x480 4:3 @ 30 fps)	1
very slow	240p (either 320x180 16:9 @ 30 fps, or 320x240 4:3 @ 30 fps)	0

Registry Path in Citrix Workspace app:

Navigate to the registry path HKEY_CURRENT_USER\SOFTWARE\Citrix\HDXMediaStream and create the following key:

Name	Type	Values	Description
OverridePerformance	DWORD	0;1;2;3	Force desired performance. Value must be in the range between 0 and 3, where 0 indicates slow and 3 fast.

For more information about Microsoft Teams optimization, see Optimization for Microsoft Teams.

Acoustic Echo Cancellation

Echo cancellation in `HdxRtcEngine.exe` can be disabled to troubleshoot audio performance issues or compatibility with peripherals that have built-in AEC capabilities.

Navigate to the registry path HKEY_CURRENT_USER\SOFTWARE\Citrix\HDXMediaStream and create the following key:

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Name: EnableAEC
Type: REG_DWORD
Data: 0
(0 disables AEC. 1 enables AEC. If Regkey isn't present, the default behavior in HdxRtcEngine is to enable AEC, irrespective of the peripheral's hardware capabilities.)

Enhancements to Microsoft Teams optimization

- Starting from Citrix Workspace app 2112.1 for Windows, the following features are available only after the future update roll-out from Microsoft Teams.

  When the update is rolled-out by Microsoft, you can check Knowledge Center articleCTX253754 for the documentation update and the announcement.

  - **Multi-window chat and meetings for Microsoft Teams**: You can use multiple windows for chat and meetings in Microsoft Teams (1.4.00.16771 or higher) when optimized by HDX in Citrix Virtual Apps and Desktops (2112 or later). You can pop out the conversations or meetings in various ways. For details on the pop-out window feature, see Microsoft Teams Pop-Out Window for Chats and Meetings on the Microsoft Office 365 site.

    If you're running an older version of Citrix Workspace app or Virtual Delivery Agent (VDA), Microsoft might deprecate the single-window code in the future. However, you can upgrade to the VDA or Citrix Workspace app version that supports multiple windows (2112 and later), before nine months after the feature is GA.

  - **App sharing**: Previously, you weren't able to share an app using the **Screen sharing** feature in Microsoft Teams when you enable the HDX™ 3D Pro policy in Citrix Studio.
    Starting with Citrix Workspace app 2112.1 for Windows and Citrix Virtual Apps and Desktops 2112, the **Screen sharing** feature allows you to share apps in Microsoft Teams. You can share an app when HDX 3D Pro policy is enabled.

  - **Give control**: You can use the **Give control** button to give control access of your shared screen to other users participating in the meeting. The other participants can make selections and modify the shared screen through keyboard, mouse, and clipboard input. Both you and the participant have control of the shared screen and you can take back the control anytime.

  - **Take control**: During screen sharing sessions, any participant can request control access through the **Request control** button. The person sharing the screen can then approve or deny the request. When you've the control, you can control the keyboard and mouse input on the screen shared and release the control to stop sharing control.

  Limitation:

© 1997–2026 Citrix Systems, Inc. All rights reserved.

The **Request control** option is not available during the peer-to-peer call between an optimized user and a user on the native Microsoft Teams desktop client that is running on the endpoint. As a workaround, users can join a meeting to get the **Request control** option.

- **Dynamic e911**: Citrix Workspace app supports dynamic emergency calling. When used in Microsoft Calling Plans, Operator Connect, and Direct Routing, it provides the option to:
  - configure and route emergency calls
  - notify security personnel

  The notification is sent based on the current location of the Citrix Workspace app that runs on the endpoint, instead of the Microsoft Teams client on the VDA.
  Ray Baum's law requires the 911 caller's dispatchable location to be transmitted to the appropriate Public Safety Answering Point (PSAP). Starting from Citrix Workspace app 2112.1 for Windows, Microsoft Teams Optimization with HDX is compliant with Ray Baum's law.

- Starting from Citrix Workspace app 2109.1 for Windows, the following features are available only after the future update roll-out from Microsoft Teams.

  When the update is rolled-out by Microsoft, you can check CTX253754 for the documentation update and the announcement.

  - **Support for WebRTC**: Citrix Workspace app 2109.1 for Windows supports WebRTC 1.0 for a better video conferencing experience along with Gallery View.
  - **Screen sharing enhancement**: You can share individual applications, windows, or full screen using the screen sharing feature in Microsoft Teams. Citrix Virtual Delivery Agent 2109 is a prerequisite for this feature.
  - **App Protection compatibility**: When App Protection is enabled, you can now share content through Microsoft Teams with HDX optimization. With this feature, you can share an application window running in the virtual desktop. Citrix Virtual Delivery Agent 2109 is a prerequisite for this feature.

  > **Note:**
  >
  > Full monitor or desktop sharing is disabled when App Protection is enabled for the delivery group.

  - **Live captions**: Citrix Workspace app 2109.1 for Windows supports real-time transcription of what the speaker is saying when Live Captions is enabled in Microsoft Teams.
  - Citrix Workspace app 2109.1 for Windows supports the following in an optimized Microsoft Teams on VM hosted apps:
    - peer-to-peer audio and video call
    - conference call

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- screen sharing

- Starting from Citrix Workspace app 2106 for Windows:
  - when the Desktop Viewer is in full-screen mode, the user can select one from all the screens covered by the Desktop Viewer to share. In window mode, the user can share the Desktop Viewer window. In seamless mode, the user can select one from all the screens to share. When the Desktop Viewer changes the window mode (maximized, restore, or minimize), the screen share stops.
- Starting from Citrix Workspace app 2105 for Windows:
  - You can configure a preferred network interface for media traffic.

    Navigate to `\HKEY_CURRENT_USER\SOFTWARE\Citrix\HDXMediaStream` and create a key called `NetworkPreference`(REG_DWORD).

    Select one of the following values as required:

    - 1: Ethernet
    - 2: Wi-Fi
    - 3: Cellular
    - 5: Loopback
    - 6: Any

    By default and if no value is set, the WebRTC media engine chooses the best available route.
  - You can disable the audio device module 2 (ADM2) so that the legacy Audio Device Module (ADM) is used for quad-channel microphones. Disabling ADM2 helps in resolving issues related to microphones in a call.

    To disable ADM2, navigate to `\HKEY_CURRENT_USER\SOFTWARE\Citrix\HDXMediaStream` and create a key named `DisableADM2` (REG_DWORD) and set the value to 1.
- Starting from Citrix Workspace app 2103.1 for Windows:
  - The VP9 video codec is now disabled by default.
  - Enhancement to echo cancellation, auto gain control, noise suppression configurations: If Microsoft Teams configures these options, Citrix-redirected Microsoft Teams honors the values as configured. Otherwise, these options are set to **True** by default.
  - `DirectWShow` is now the default renderer.

    To change the default renderer, do the following:

    1. Launch the Registry editor.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

2. Navigate to the following key location: `HKEY_CURRENT_USER\SOFTWARE\Citrix\HDXMediaStream`.
3. Update the following value: `"UseDirectShowRendererAsPrimary"=dword:00000000`

   Other possible values:

   - 0: Media Foundation
   - 1: DirectShow (Default)
4. Relaunch the Citrix Workspace app.

- Starting from Citrix Workspace app 2012 for Windows:
  - Peers can now see the presenter's mouse pointer in a screen sharing session.
  - The WebRTC media engine now honors the proxy server configured on the client device.
- Starting from Citrix Workspace app 2009.6 for Windows:
  - Microsoft Teams displays previously used peripheral devices in the **Preferred devices** list.
  - The WebRTC media engine accurately determines the maximum encoding resolution possible on an endpoint. The WebRTC media engine estimates multiple times a day and not only on first launch.
  - The Citrix Workspace app installer is packaged with the Microsoft Teams ringtones.
  - Echo cancellation improvements - Reduced echo level when a peer has a speaker or microphone that generates an echo.
  - Screen sharing improvements - when you share your screen, only the **Desktop Viewer** screen is captured in native bitmap format. Previously, client local windows that overlaid on top of the **Desktop Viewer** window were blacked out.
- Starting from Citrix Workspace app 2002 for Windows:
  - when you share your workspace using Microsoft Teams, Citrix Workspace app displays a red border around the area of the monitor that is currently being shared. You can share only the **Desktop Viewer** window, or any local window overlaid on top of it. When you minimize the **Desktop Viewer** window, screen sharing is paused.

Administrator tasks and considerations

This article discusses the tasks and considerations that are relevant for administrators of Citrix Workspace app for Windows.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Feature flag management

If an issue occurs with Citrix Workspace app in production, we can disable an affected feature dynamically in Citrix Workspace app even after the feature is shipped.

To do so, we use feature flags and a third-party service called LaunchDarkly. You do not need to make any configurations to enable traffic to LaunchDarkly, except when you have a firewall or proxy blocking outbound traffic. In that case, you enable traffic to LaunchDarkly via specific URLs or IP addresses, depending on your policy requirements.

You can enable traffic and communication to LaunchDarkly in the following ways:

Enable traffic to the following URLs

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

List IP addresses in an allow list If you must list IP addresses in an allow list, for a list of all current IP address ranges, see LaunchDarkly public IP list. You can use this list to know that your firewall configurations are updated automatically in keeping with the infrastructure updates. For details about the status of the infrastructure changes, see the LaunchDarkly Status page.

LaunchDarkly system requirements Verify if the apps can communicate with the following services if you have split tunneling on the Citrix ADC set to **OFF** for the following services:

- LaunchDarkly service.
- APNs listener service

Disabling LaunchDarkly service You can disable the LaunchDarkly service by using a Group Policy Object (GPO) policy.

1. Open the Citrix Workspace app Group Policy Object administrative template by running gpedit.msc.
2. Under the **Computer Configuration** node, go to **Administrative Templates** > **Citrix Components** > **Citrix Workspace** > **Compliance**.
3. Select the **Disable sending data to 3rd party** policy and set it to Enabled.
4. Click **Apply** and **OK**.

You can also disable the LaunchDarkly service using the registry.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

1. Open the registry editor.
2. Navigate to `HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Citrix` on 64-bit machine and `HKEY_LOCAL_MACHINE\SOFTWARE\Citrix` on 32-bit machine.
3. Create and add a registry string REG_SZ with the name as **EnableLDFeature** and set its value as **False**.
4. Exit and restart Citrix Workspace app for the changes to take effect.

App Protection

> **Disclaimer**
>
> App Protection policies filter the access to required functions of the underlying operating system (specific API calls required to capture screens or keyboard presses). App Protection policies provide protection even against custom and purpose-built hacker tools. However, as operating systems evolve, new ways of capturing screens and logging keys might emerge. While we continue to identify and address them, we cannot guarantee full protection in specific configurations and deployments.

App Protection is an add-on feature that provides enhanced security when using Citrix Virtual Apps and Desktops and Citrix DaaS (formerly Citrix Virtual Apps and Desktops service). The feature restricts the ability of clients to compromise with keylogging and screen capturing malware. App Protection prevents exfiltration of confidential information such as user credentials and sensitive information on the screen. The feature prevents users and attackers from taking screenshots and from using keyloggers to glean and exploit sensitive information.

App Protection requires that you install an add-on license on your License Server. A Citrix Virtual Desktops license must also be present. For information on Licensing, see the Configure section in the App Protection documentation.

Requirements:

- Citrix Virtual Apps and Desktops™ Version 1912 or later.
- StoreFront Version 1912.
- Citrix Workspace app Version 1912 or later.

Prerequisites:

- The App Protection feature must be enabled on the Controller. For more information, see App Protection documentation.

You can include the App Protection component with Citrix Workspace app either:

- During Citrix Workspace app installation using the command-line interface or the GUI OR
- During an app launch (on-demand installation).

© 1997–2026 Citrix Systems, Inc. All rights reserved.

> **Note:**
>
> - This feature is supported only on desktop operating systems such as Windows 10, Windows 8.1.
> - Starting with Version 2006.1, Citrix Workspace app isn't supported on Windows 7. So, App Protection doesn't work on Windows 7. For more information, see Deprecation.
> - This feature isn't supported over Remote Desktop Protocol (RDP).

On-premises HDX session protection:

Two policies provide anti-keylogging and anti-screen-capturing functionality in a session. These policies must be configured through PowerShell. No GUI is available for the purpose.

> **Note:**
>
> Starting with Version 2103, Citrix DaaS supports App Protection with StoreFront only.

For information on App Protection configuration on Citrix Virtual Apps and Desktops, see App Protection documentation.

App Protection - Configuration in Citrix Workspace app

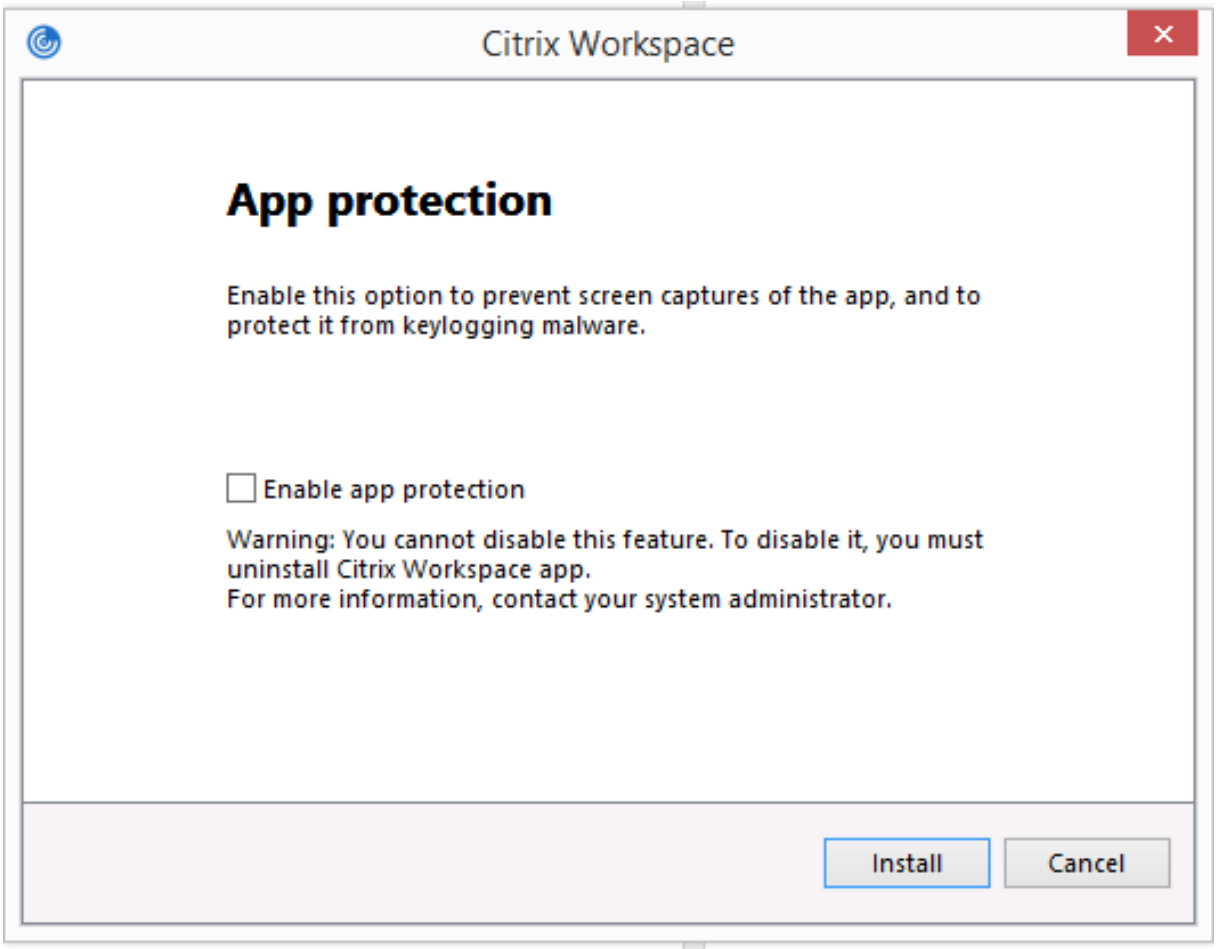
> **Note:**
>
> - Include the App Protection component with Citrix Workspace app only if your administrator has instructed you to do so.
> - Adding the App Protection component might impact the screen-capturing capabilities on your device.

During the Citrix Workspace app installation, you can include App Protection using one of the following methods:

- GUI
- Command-line interface

GUI During the Citrix Workspace app installation, use the following dialog to include the App Protection component. Select **Enable app protection** and then click **Install** to continue with the installation.

© 1997–2026 Citrix Systems, Inc. All rights reserved.



> **Note:**
>
> Not enabling App Protection during installation causes a prompt to appear when you launch a protected app. Follow the prompt to install the App Protection component.

Command-line interface Use the command-line switch `/includeappprotection` during Citrix Workspace app installation to add the App Protection component.

The following table provides information on screens protected depending on deployment:

App Protection deployment	Screens protected	Screens not protected
Included in Citrix Workspace app	Self-Service plug-in and Auth manager / User credentials dialog	Connection Center, Devices, Any Citrix Workspace app error messages, Auto client reconnect, Add account

© 1997–2026 Citrix Systems, Inc. All rights reserved.

App Protection deployment	Screens protected	Screens not protected
Configured on the Controller	ICA session screen (both apps and desktops)	Connection Center, Devices, Any Citrix Workspace app error messages, Auto client reconnect, Add account

In earlier releases, the entire screen including the non-protected apps in the background used to black out, when taking a screenshot of a protected window.

Starting with Version 2008, when you're taking a screenshot, only the protected window is blacked out. You can take a screenshot of the area outside the protected window.

Expected Behavior:

The expected behavior depends upon the method by which users access the StoreFront that has the protected resources.

> **Note:**
>
> - Citrix recommends that you only use the native Citrix Workspace app to launch a protected session.

- **Behavior on the workspace for web:**

  The App Protection component isn't supported on the workspace for web configurations. Applications that are protected by App Protection policies aren't enumerated. For more information about the resources assigned, contact your system administrator.

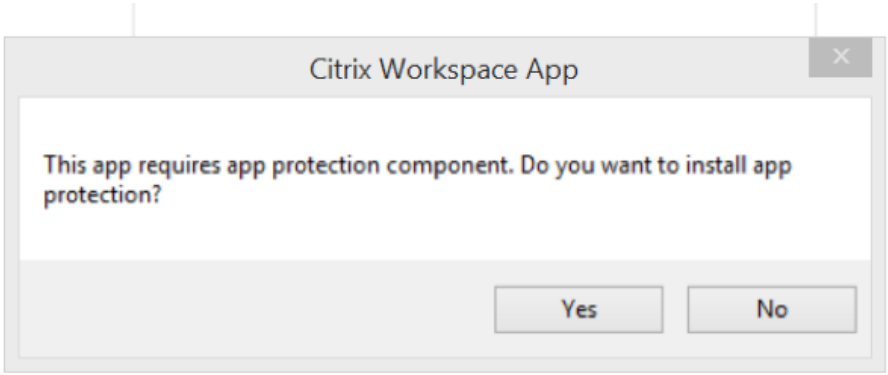
- **Behavior on Citrix Workspace app versions that do not support App Protection:**

  On Citrix Workspace app Version 1911 and earlier, applications that are protected by App Protection policies aren't enumerated on StoreFront.

- **Behavior of apps that have the App Protection feature configured on the Controller:**

  On an App Protection configured-Controller, if you try to launch an application that is protected, the App Protection is installed on-demand. The following dialog appears:

© 1997–2026 Citrix Systems, Inc. All rights reserved.



Click **Yes** to install the App Protection component. You can then launch the protected app.

- **Behavior of protected session in case of Remote Desktop Protocol(RDP)**
  - Your active protected session disconnects, if you launch a Remote Desktop Protocol(RDP) session.
  - You can't launch a protected session in a Remote Desktop Protocol(RDP) session.

Enhancement to App Protection configuration

Previously, the authentication manager and the **Self-Service plug-in** dialogs were protected by default.

Starting with Version 2012, you can configure the anti-keylogging and anti-screen-capturing functionalities separately for both the authentication manager and Self-Service plug-in interfaces. You can configure the functionalities by using a Group Policy Object (GPO) policy.

> **Note:**
>
> This GPO policy isn't applicable for ICA and SaaS sessions. The ICA and SaaS sessions continue to be controlled using the Delivery Controller™ and Citrix Gateway Service.

Configuring App Protection for the Self-Service plug-in interface:

1. Open the Citrix Workspace app Group Policy Object administrative template by running `gpedit.msc`.
2. Under the **Computer Configuration** node, go to **Administrative Templates** > **Citrix Components** > **Citrix Workspace**.
3. To configure anti-keylogging and anti-screen-capturing for the Self-Service plug-in dialog, select **Self Service** > **Manage app protection** policy.
4. Select one or both the following options:

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- **Anti-key logging**: Prevents keyloggers from capturing keystrokes.
- **Anti-screen-capturing**: Prevents users from taking screenshots and sharing their screen.

5. Click **Apply** and **OK**.

Configuring App Protection for authentication manager:

1. Open the Citrix Workspace app Group Policy Object administrative template by running `gpedit.msc`.
2. Under the **Computer Configuration** node, go to **Administrative Templates** > **Citrix Components** > **Citrix Workspace**.
3. To configure anti-keylogging and anti-screen-capturing for the authentication manager, select **User authentication** > **Manage app protection** policy.
4. Select one or both the following options:

   - **Anti-key logging**: Prevents keyloggers from capturing keystrokes.
   - **Anti-screen-capturing**: Prevents users from taking screenshots and sharing their screen.

5. Click **Apply** and **OK**.

App Protection error logs:

Starting with Version 2103, the App Protection logs are collected as part of bthe Citrix Workspace app logs. For more information about log collection, see Log collection.

You do not need to install or use a third-party app to collect the App Protection logs specifically. However, DebugView can still be continued to be used for log collection.

The App Protection logs are registered to the debug output. To collect these logs, do the following:

1. Download and install the DebugView app from the Microsoft website.
2. Launch the command prompt and run the following command:

   ```
   Dbgview.exe /t /k /v /l C:\logs.txt
   ```

   From the example above, you can view the logs in `log.txt` file.

The command indicates the following:

- `/t` –The DebugView app starts minimized in the notification area.
- `/k` –Enable kernel capture.
- `/v` –Enable verbose kernel capture.
- `/l` –Log the output to a specific file.

Uninstalling the App Protection component:

To uninstall the App Protection component, you must uninstall Citrix Workspace app from your system. Restart the system for the changes to take effect.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

> **Note:**
>
> App Protection is supported only on upgrade from Version 1912 onwards.

Known issues or limitations:

- This feature isn't supported on Microsoft Server operating systems such as Windows Server 2012 R2 and Windows Server 2016.
- This feature isn't supported in double-hop scenarios.
- For this feature to function properly, disable the **Client clipboard redirection** policy on the VDA.

Application Categories

Application Categories allow users to manage collections of applications in Citrix Workspace app. You can create application groups for applications shared across different delivery groups or used by a subset of users within delivery groups.

For more information, see Create application groups in the Citrix Virtual Apps and Desktops documentation.

Improved ICA® file security

This feature provides enhanced security while handling ICA files during a Virtual Apps and Desktops session launch.

Citrix Workspace app lets you store the ICA file in the system memory instead of the local disk when you launch a virtual apps and desktops session.

This feature aims to eliminate surface attacks and any malware that might misuse the ICA file when stored locally. This feature is also applicable on virtual apps and desktops sessions that are launched on workspace for Web

Configuration

ICA file security is also supported when Citrix Workspace or StoreFront is accessed through the web. Client detection is a prerequisite for the feature to work if it's accessed through the web. If you're accessing StoreFront using a browser, enable the following attributes in the web.config file on StoreFront deployments:

© 1997–2026 Citrix Systems, Inc. All rights reserved.

StoreFront Version	Attribute
2.x	pluginassistant
3.x	protocolHandler

When you sign in to the store through the browser, click **Detect Workspace App**. If the prompt doesn't appear, clear the browser cookies and try again.

If it's a Workspace deployment, you can find the client detection settings by navigating to **Accounts settings** > **Advanced** > **Apps and Desktops Launch Preference**.

You can take extra measures so that sessions are launched only using the ICA file stored on system memory. Use any of the following methods:

- Group Policy Object (GPO) Administrative template on the client.
- Global App Config Service.
- Workspace for web.

Using the GPO:

To block session launches from ICA files that are stored on the local disk, do the following:

1. Open the Citrix Workspace app Group Policy Object administrative template by running `gpedit.msc`.
2. Under the **Computer Configuration** node, go to **Administrative Templates** > **Citrix Components** > **Citrix Workspace** > **Client Engine**.
3. Select the **Secure ICA file session launch** policy and set it to **Enabled**.
4. Click **Apply** and **OK**.

Using the Global App Config Service:

To block session launches from ICA files that are stored on the local disk, do the following:

Set the **Block Direct ICA File Launches** attribute to **True**.

For more information about Global App Config Service, see the Global App Config Service documentation.

Using workspace for web:

To disallow ICA file download on the local disk when using Workspace for Web, do the following:

Run the PowerShell module. See Configure DisallowICADownload.

> **Note:**

© 1997–2026 Citrix Systems, Inc. All rights reserved.

> The **DisallowICADownload** policy isn't available for StoreFront deployments.

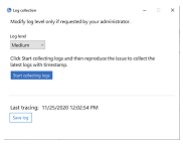
Log collection

Log collection simplifies the process of collecting logs for Citrix Workspace app. The logs help Citrix to troubleshoot, and, in cases of complicated issues, provides support.

You can collect logs using the GUI.

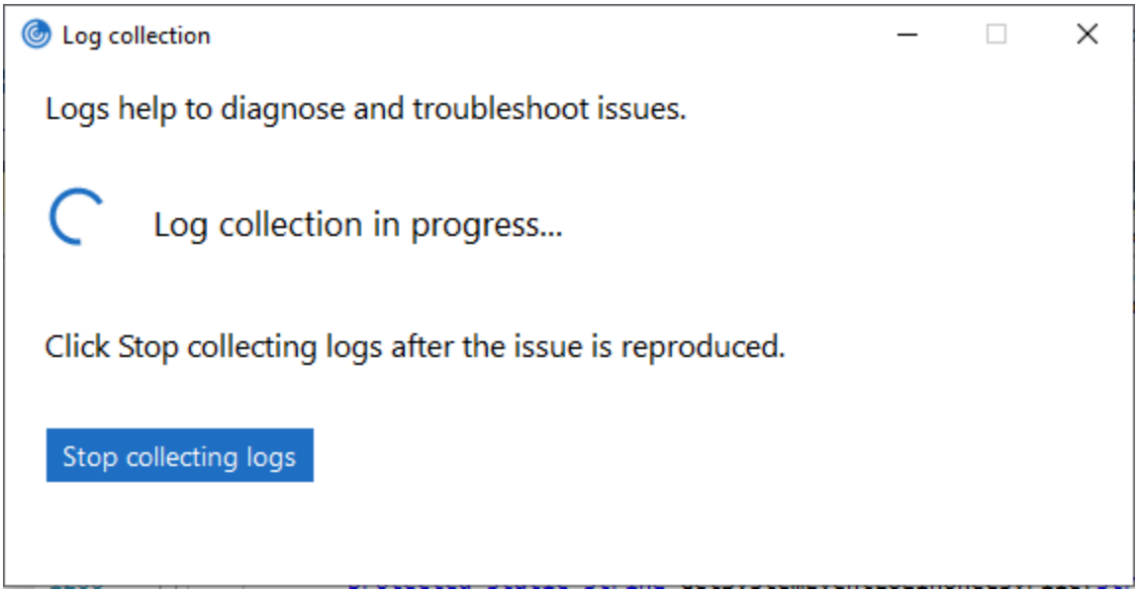
Collecting logs:

1. Right-click the Citrix Workspace app icon in the notification area and select **Advanced Preferences**.
2. Select **Log collection**.
   The Log collection dialog appears.



3. Select one of the following log levels:
   - Low
   - Medium
   - Verbose
4. Click **Start collecting logs** to reproduce the issue and collect the latest logs.

   The log collection process starts.



© 1997–2026 Citrix Systems, Inc. All rights reserved.

5. Click **Stop collecting logs** after the issue is reproduced.
6. Click **Save log** to save the logs to a desired location.

HDX adaptive throughput

HDX adaptive throughput intelligently fine-tunes the peak throughput of the ICA session by adjusting output buffers. The number of output buffers is initially set at a high value. This high value allows data to be transmitted to the client more quickly and efficiently, especially in high latency networks.

It provides better interactivity, faster file transfers, smoother video playback, higher framerate, and resolution results in an enhanced user experience.

Session interactivity is constantly measured to determine whether any data streams within the ICA session are adversely affecting interactivity. If that occurs, the throughput is decreased to reduce the impact of the large data stream on the session and allow interactivity to recover.

This feature is supported only on Citrix Workspace app 1811 for Windows and later.

> **Important:**
>
> HDX adaptive throughput changes the output buffers by moving the mechanism from the client to the VDA. So, adjust the number of output buffers on the client as needed..

Adaptive transport

Adaptive Transport is a mechanism in Citrix Virtual Apps and Desktops and Citrix DaaS that allows to use Enlightened Data Transport (EDT) protocol for ICA connections. For more information, see Adaptive transport section in the Citrix Virtual Apps and Desktops documentation.

Advanced Preferences sheet

Starting with Version 4.10, you can customize the **Advanced Preferences** sheet's availability and contents present in the right-click menu of the Citrix Workspace app icon in the notification area. Doing so ensures that users can apply only administrator-specified settings on their systems. Specifically, you can:

- Hide the Advanced Preferences sheet altogether
- Hide the following specific settings from the sheet:
    - Data collection
    - Connection Center
    - Configuration checker

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- Keyboard and Language bar
- High DPI
- Support information
- Shortcuts and Reconnect
- Citrix Casting™

Hiding Advanced Preferences option from the right-click menu

You can hide the Advanced Preferences sheet by using the Citrix Workspace app Group Policy Object (GPO) administrative template:

1. Open the Citrix Workspace app Group Policy Object administrative template by running gpedit.msc.
2. Under the **Computer Configuration** node, go to **Administrative Templates** > **Citrix Workspace** > **Self Service** > **Advanced Preferences Options**.
3. Select the **Disable Advance Preferences** policy.
4. Select **Enabled** to hide the Advanced Preferences option from the right-click menu of the Citrix Workspace app icon in the notification area.

> **Note:**
>
> By default, the **Not Configured** option is selected.

Hiding specific settings from the Advanced Preferences sheet

You can hide specific user-configurable settings from the **Advanced Preferences** sheet by using the Citrix Workspace app Group Policy Object administrative template. To hide the settings:

1. Open the Citrix Workspace app Group Policy Object administrative template by running gpedit.msc.
2. Under the **Computer Configuration** node, go to **Administrative Templates** > **Citrix Workspace** > **Self Service** > **Advanced Preferences Options**.
3. Select the policy for the setting that you want to hide.

The following table lists the options that you can select and the effects of each:

Options	Action
Not Configured	Displays the setting
Enabled	Hides the setting
Disabled	Displays the setting

© 1997–2026 Citrix Systems, Inc. All rights reserved.

You can hide the following specific settings from the Advanced Preferences sheet:

- Configuration checker
- Connection Center
- High DPI
- Data collection
- Delete saved passwords
- Keyboard and Language bar
- Shortcuts and Reconnect
- Support information
- Citrix Casting

Hiding the Reset Workspace option from the Advanced Preferences sheet using the Registry editor

You can hide the **Reset Workspace** option from the Advanced Preferences sheet only using the Registry editor.

1. Launch the registry editor.
2. Navigate to `HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\Dazzle`.
3. Create a String Value key **EnableFactoryReset** and set it to any of the following options:
    - True - Displays the Reset Workspace option in the Advanced Preferences sheet.
    - False - Hides the Reset Workspace option in the Advanced Preferences sheet.

Hiding Citrix Workspace Updates option from the Advanced Preferences sheet

> **Note:**
>
> The policy path for the Citrix Workspace Updates option is different from the other options present in the Advanced Preferences sheet.

1. Open the Citrix Workspace app Group Policy Object administrative template by running gpedit.msc.
2. Under the **Computer Configuration** node, go to **Administrative Templates** > **Citrix Components** > **Citrix Workspace** > **Workspace Updates**.
3. Select the **Workspace Updates** policy.
4. Select **Disabled** to hide the Workspace Updates settings from the **Advanced Preferences** sheet.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

StoreFront to cloud store URL Migration

This feature is in Technical Preview. StoreFront to cloud store URL migration enables you to seamlessly migrate your end users from a StoreFront store to Workspace store with minimal user interaction.

Consider, all your end users have a StoreFront store `storefront.com` added to their Citrix Workspace app. As an administrator, you can configure a StoreFront URL to cloud store URL Mapping { 'storefront.com':'xyz.cloud.com'} in the Global App Configuration Service. The Global App Config Service pushes the setting to all Citrix Workspace app instances, on both managed and unmanaged devices that have the StoreFront URL `storefront.com` added.

Once the setting is detected, Citrix Workspace app adds the mapped cloud store URL `xyz.cloud.com` as another store. When the end user launches the Citrix Workspace app, the Citrix Workspace store opens. The previously added StoreFront store `storefront.com` remains added to the Citrix Workspace app. Users can always switch back to the StoreFront store `storefront.com` using the **Switch Accounts** option in the Citrix Workspace app. Admins can control the removal of the StoreFront store `storefront.com` from the Citrix Workspace app at the users'end points. The removal can be done through the global app config service.

To enable the feature, do the following steps:

1. Configure StoreFront to Workspace mapping using the Global App Config Service. For more information on the Global App config service, see Global App Configuration Service.
2. Edit the payload in the app config service:

```
{
  "serviceURL": Unknown macro: \{
  "url" }

,
"settings":{

"name":"Productivity Apps", [New Store Name]
"description":"Provides access StoreFront to Workspace Migration",
"useForAppConfig":true,
"appSettings":
{
  "windows":[ Unknown macro: \{
  "category" }

]
 }

 }

 }
```

© 1997–2026 Citrix Systems, Inc. All rights reserved.

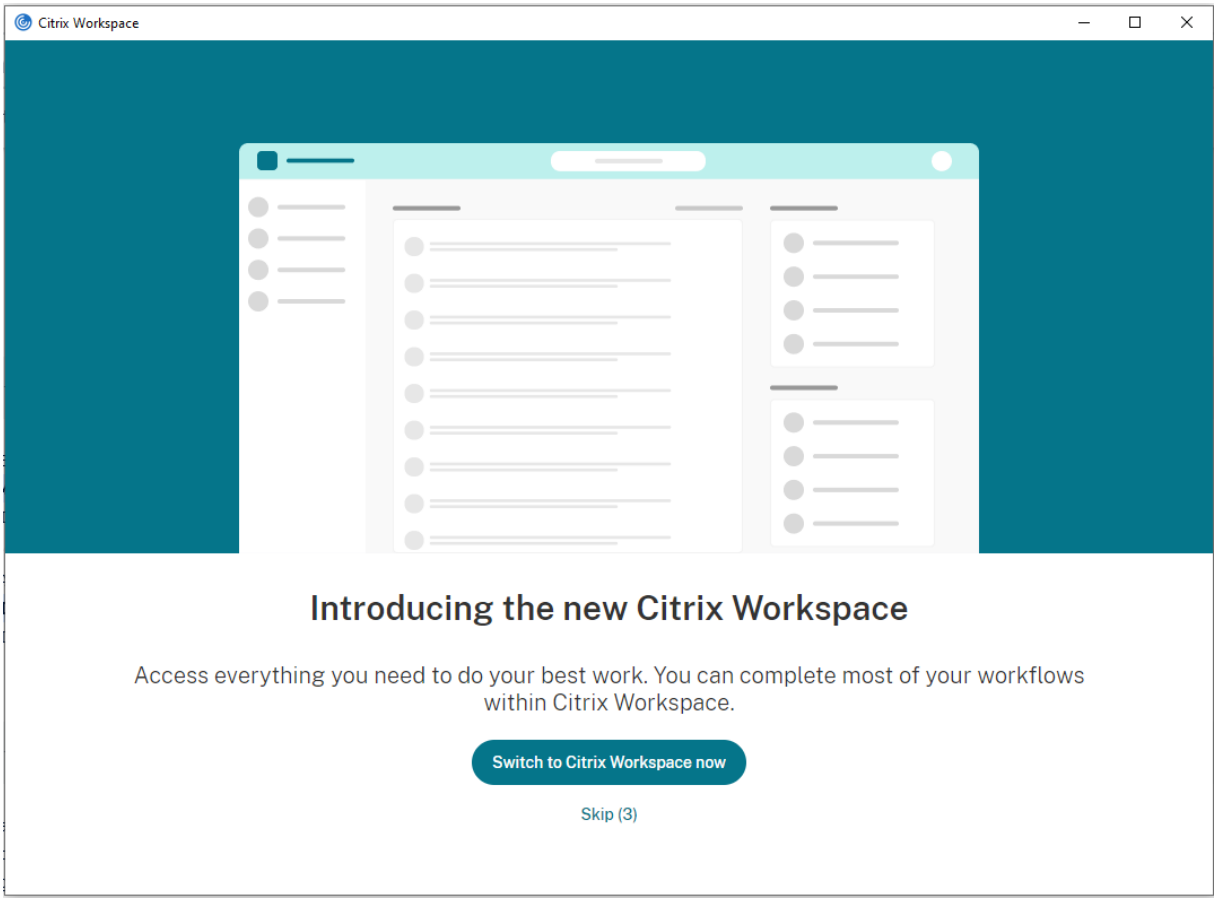
> **Note:**
>
> If you're configuring the payload for the first time, use POST.
> If you're editing the existing payload configuration, use PUT and check that you have the payload that consists of all the supported settings.

3. Specify the StoreFront URL `storefront.com` as the value for **URL** in the **serviceURL** section.
4. Configure the cloud store URL `xyz.cloud.com` inside the section **migrationUrl**.
5. Use **storeFrontValidUntil** to set the timeline for the removal of the StoreFront store from the Citrix Workspace app. This field is optional. You can set the following value based on your requirement:

   - Valid date in the format (YYYY-MM-DD)

   > **Note:**
   >
   > If you have provided a past date, then the StoreFront store is removed immediately upon URL migration. If you have provided a future date, then the StoreFront store is removed on the set date.

Once the settings are pushed, the following screen appears:



© 1997–2026 Citrix Systems, Inc. All rights reserved.

When the user clicks **Switch to Citrix Workspace now**, the cloud store URL is added to Citrix Workspace app and the authentication prompt appears. Users have a limited option to delay the transition up to three times.

Application delivery

When delivering applications with Citrix Virtual Apps and Desktops and Citrix DaaS, consider the following options to enhance the user experience:

- Web Access Mode - Without any configuration, Citrix Workspace app provides browser-based access to applications and desktops. You can open a browser to a Workspace for web to select and use the applications you want. In this mode, no shortcuts are placed on the user's desktop.
- Self-Service Mode - By adding a StoreFront account to Citrix Workspace app or configuring Citrix Workspace app to point to a StoreFront website, you can configure *self-service mode*. Self-Service mode allows you to subscribe to applications from the Citrix Workspace app user interface. The enhanced user experience is similar to that of a mobile app store. In a self-service mode, you can configure mandatory, auto-provisioned, and featured app keyword settings as required.

> **Note:**
>
> By default, Citrix Workspace app allows you to select the applications to display in the Start menu.

- App shortcut-only mode - Administrators can configure Citrix Workspace app to automatically place application and desktop shortcuts directly in the Start menu or on the desktop. The placement is similar to Citrix Workspace app Enterprise. The new *shortcut only* mode allows you to find all the published apps within the familiar Windows navigation schema where you would expect to find them.

For more information, see the Create Delivery Groups section in the Citrix Virtual Apps and Desktops documentation.

Configure self-service mode

By simply adding a StoreFront account to Citrix Workspace app or configuring Citrix Workspace app to point to a StoreFront site, you can configure self-service mode. The configuration allows users to subscribe to applications from the Citrix Workspace user interface. The enhanced user experience is similar to that of a mobile app store.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

> **Note:**
>
> By default, Citrix Workspace app allows users to select the applications they want to display in their Start menu.

In self-service mode, you can configure mandatory, auto-provisioned, and featured app keyword settings as needed.

Append keywords to the descriptions that you provide for delivery group applications:

- To make an individual app mandatory, so that it cannot be removed from Citrix Workspace app, append the string KEYWORDS: Mandatory to the application description. There is no Remove option for users to unsubscribe to mandatory apps.
- To automatically subscribe all users of a store to an application, append the string KEYWORDS: Auto to the description. When users log on to the store, the application is automatically provisioned without users needing to manually subscribe to the application.
- To advertise applications to users or to make commonly used applications easier to find by listing them in the Citrix Workspace Featured list, append the string KEYWORDS: Featured to the application description.

Customize the app shortcut location using the Group Policy Object template

1. Open the Citrix Workspace app Group Policy Object administrative template by running gpedit.msc.
2. Under the **Computer Configuration** node, go to **Administrative Templates** > **Citrix Components** > **Citrix Workspace** > **Self Service**.
3. Select the **Manage SelfServiceMode** policy.
    a) Select **Enabled** to view the Self-service user interface.
    b) Select **Disabled** to subscribe to the apps manually. This option hides the Self-service user interface.
4. Select the **Manage App Shortcut** policy.
5. Select the options as required.
6. Click **Apply** and **OK**.
7. Restart Citrix Workspace app for the changes to take effect.

Using StoreFront account settings to customize app shortcut locations

You can set up shortcuts in the Start menu and on the desktop from the StoreFront site. The following settings can be added in the web.config file in `C:\inetpub\wwwroot\Citrix\Roaming`in the **<annotatedServices>** section:

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- To put shortcuts on the desktop, use PutShortcutsOnDesktop. Settings: "true"or "false"(default is false).
- To put shortcuts in the Start menu, use PutShortcutsInStartMenu. Settings: "true"or "false" (default is true).
- To use the category path in the Start menu, use UseCategoryAsStartMenuPath. Settings: "true" or "false"(default is true).

> **Note:**
>
> Windows 8, 8.1 and Windows 10 do not allow the creation of nested folders within the Start menu. Instead, display the applications individually or under the root folder. Applications are not within the Category sub folders defined with Citrix Virtual Apps and Desktops.

- To set a single directory for all shortcuts in the Start menu, use `StartMenuDir`. Setting: String value, being the name of the folder into which shortcuts are written.
- To reinstall modified apps, use AutoReinstallModifiedApps. Settings: "true"or "false"(default is true).
- To show a single directory for all shortcuts on the desktop, use `DesktopDir`. Setting: String value, being the name of the folder into which shortcuts are written.
- To not create an entry on the clients 'add/remove programs', use `DontCreateAddRemoveEntry`. Settings: "true"or "false"(default is false).
- To remove shortcuts and Citrix Workspace icon for an application that was previously available from the Store but now is not available, use `SilentlyUninstallRemovedResources`. Settings: "true"or "false"(default is false).

In the web.config file, add the changes in the **XML** section for the account. Find this section by locating the opening tab:

```
<account id=... name="Store"
```

The section ends with the </account> tag.

Before the end of the account section, in the first properties section:

```
<properties> <clear> <properties>
```

Properties can be added into this section after the <clear /> tag, one per line, giving the name and value. For example:

```
<property name="PutShortcutsOnDesktop"value="True"/>
```

> **Note:**
>
> Property elements added before the <clear /> tag might invalidate them. Removing the <clear /> tag when adding a property name and value is optional.

An extended example for this section is:

© 1997–2026 Citrix Systems, Inc. All rights reserved.

```
<properties <property name="PutShortcutsOnDesktop"value="True"<
property name="DesktopDir"value="Citrix Applications">
```

> **Important**
>
> In multiple server deployments, use only one server at a time to change the configuration of the server group. Ensure that the Citrix StoreFront management console is not running on any of the other servers in the deployment. Once complete, propagate your configuration changes to the server group, so that the other servers in the deployment are updated. For more information, see StoreFront documentation.

Using per-app settings in Citrix Virtual Apps and Desktops 7.x to customize app shortcut locations

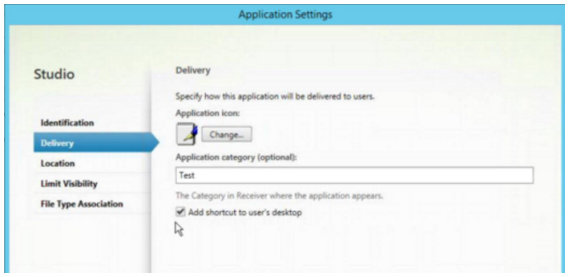
Citrix Workspace app can be configured to automatically place application and desktop shortcuts directly in the Start menu or on the desktop. However, this configuration is similar to the previous Workspace for Windows versions. However, release 4.2.100 introduced the ability to control the placement of the app-shortcut using Citrix Virtual Apps per app settings. The functionality is useful in environments with a handful of applications that need to be displayed in consistent locations.

Using per app settings in XenApp 7.6 to customize app shortcut locations

To configure a per app publishing shortcut in XenApp 7.6:

1. In Citrix Studio, locate the **Application Settings** screen.
2. In the **Application Settings** screen, select **Delivery**. Using this screen, you can specify how applications are delivered to users.
3. Select the appropriate icon for the application. Click **Change** to browse to the location of the required icon.
4. In the **Application category** field, optionally specify the category in Citrix Workspace app where the application appears. For example, if you are adding shortcuts to Microsoft Office applications, enter Microsoft Office.
5. Select the **Add shortcut to user's desktop** checkbox.
6. Click OK.

© 1997–2026 Citrix Systems, Inc. All rights reserved.



Reducing enumeration delays or digitally signing application stubs

Citrix Workspace app provides functionality to copy the .EXE stubs from a network share, if:

- there is a delay in app enumeration at each sign-in, or
- there is a need to sign application stubs digitally.

This functionality involves several steps:

1. Create the application stubs on the client machine.
2. Copy the application stubs to a common location accessible from a network share.
3. If necessary, prepare an allow list (or, sign the stubs with an Enterprise certificate.
4. Add a registry key to enable Workspace for Windows to create the stubs by copying them from the network share.

If **RemoveappsOnLogoff** and **RemoveAppsonExit** are enabled, and users are experiencing delays in app enumeration at every logon, use the following workaround to reduce the delays:

1. Use regedit to add `HKEY_CURRENT_USER\Software\Citrix\Dazzle` /v ReuseStubs /t REG_SZ /d “true”.
2. Use regedit to add `HKEY_LOCAL_MACHINE\Software\Citrix\Dazzle` /v ReuseStubs /t REG_SZ /d “true”. HKEY_CURRENT_USER has preference over HKEY_LOCAL_MACHINE.

> **Caution**
>
> Editing the registry incorrectly can cause serious problems that might require you to reinstall your operating system. Citrix cannot guarantee that problems resulting from the incorrect use of the Registry Editor can be solved. Use the Registry Editor at your own risk. Be sure to back up the registry before you edit it.

Enable a machine to use pre-created stub executables that are stored on a network share:

1. On a client machine, create stub executables for all apps. To accomplish create stub executables, add all the applications to the machine using Citrix Workspace app. Citrix Workspace app generates the executables.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

2. Harvest the stub executables from %APPDATA%\Citrix\SelfService. You only need the .exe files.
3. Copy the executables to a network share.
4. For each client machine that is locked down, set the following registry keys:

    a) Reg add HKEY_LOCAL_MACHINE\Software\Citrix\Dazzle /v CommonStubDirectory /t REG_SZ /d "\\ShareOne\WorkspaceStubs"
    b) Reg add HKEY_LOCAL_MACHINE\Software\Citrix\Dazzle /v
    c) CopyStubsFromCommonStubDirectory /t REG_SZ /d "true". It's also possible to configure these settings on HKEY_CURRENT_USER if you prefer. HKEY_CURRENT_USER has preference over HKEY_LOCAL_MACHINE.
    d) Exit and restart Citrix Workspace app for the changes to take effect.

Example use cases:

This topic provides use cases for app shortcuts.

Allowing users to choose what they want in the Start menu (Self-Service)

If you have dozens or even hundreds of apps, allow users to select the applications to add to **Favorite** and **Start** menu:

If you want the user to choose the applications that they want in their Start menu.	configure Citrix Workspace app in self-service mode. In this mode, you also configure *auto-provisioned* and *mandatory* app keyword settings as needed.
If you want the user to choose the applications that they want in their Start menu but also want specific app shortcuts on the desktop.	configure Citrix Workspace app without any options and then use per app settings for the few apps that you want on the desktop. Use *auto provisioned* and *mandatory* apps as needed.

No app shortcuts in the Start menu

If a user has a family computer, you might not need or want app shortcuts at all. In such scenarios, the simplest approach is browser access; install Citrix Workspace app without any configuration and browse to workspace for web. You can also configure Citrix Workspace app for self-service access without putting shortcuts anywhere.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

If you want to prevent Citrix Workspace app from putting application shortcuts in the Start menu automatically.	configure Citrix Workspace app with PutShortcutsInStartMenu=False. Citrix Workspace app doesn't put apps in the Start menu even in self-service mode unless you put them using per app settings.

All app shortcuts in the Start menu or on the Desktop

If the user has only a few apps, put them all in the Start menu or on the desktop, or in a folder on the desktop.

If you want Citrix Workspace app to put all application shortcuts in the start menu automatically.	configure Citrix Workspace app with SelfServiceMode =False. All available apps appear in the Start menu.
If you want all application shortcuts to put on the desktop.	configure Citrix Workspace app with PutShortcutsOnDesktop = true. All available apps appear on the desktop.
If you want all shortcuts to be put on the desktop in a folder.	configure Citrix Workspace app with DesktopDir=Name of the desktop folder where you want applications.

Per app settings in XenApp 6.5 or 7.x

If you want to set the location of shortcuts so every user finds them in the same place use XenApp® per App Settings:

If you want per app settings to determine where applications are placed independently of whether in self-service mode or Start menu mode.	configure Citrix Workspace app with PutShortcutsInStartMenu=false and enable per app settings.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Apps in category folders or in specific folders

If you want applications displayed in specific folders use the following options:

If you want the application shortcuts Citrix Workspace app places in the start menu to be shown in their associated category (folder).	configure Citrix Workspace app with UseCategoryAsStartMenuPath=True.
If you want the applications that Citrix Workspace app puts in the Start menu to be in a specific folder.	configure Citrix Workspace app with StartMenuDir=the name of the Start menu folder name.

Remove apps on logoff or exit

If you don't want users to see apps while another user shares the end point, you can remove the apps when the user logs off and exits.

If you want Citrix Workspace app to remove all apps on logoff.	configure Citrix Workspace app with RemoveAppsOnLogoff=True.
If you want Citrix Workspace app to remove apps on exit.	configure Citrix Workspace app with RemoveAppsOnExit=True.

Configuring Local App Access applications

When configuring Local App Access applications:

- To specify that a locally installed application must be used instead of an application available in Citrix Workspace app, append the text string KEYWORDS:prefer="pattern."This feature is referred to as Local App Access.

  Before you install an application on a user's computer, Citrix Workspace app searches for the specified patterns to determine if the application is installed locally. If it is, Citrix Workspace app subscribes the application and does not create a shortcut. When the user starts the application from the Citrix Workspace app window, Citrix Workspace app starts the locally installed (preferred) application.

  If a user uninstalls a preferred application outside of Citrix Workspace app, the application is unsubscribed during the next Citrix Workspace app refresh. If a user uninstalls a preferred applica-

© 1997–2026 Citrix Systems, Inc. All rights reserved.

tion from the Citrix Workspace app dialog, Citrix Workspace app unsubscribes the application but does not uninstall it.

> **Note:**
>
> The keyword prefer is applied when Citrix Workspace app subscribes an application. Adding the keyword after the application is subscribed has no effect.

You can specify the preferred keyword multiple times for an application. Only one match is needed to apply the keyword to an application. The following patterns can be used in any combination:

- To specify that a locally installed application must be used instead of an application available in Citrix Workspace app, append the text string KEYWORDS:prefer="pattern". This feature is referred to as Local App Access.

  Before you install an application on a user's computer, Citrix Workspace app searches for the specified patterns to determine if the application is installed locally. If it is, Citrix Workspace app subscribes the application and does not create a shortcut. When the user starts the application from the Citrix Workspace app dialog, Citrix Workspace app starts the locally installed (preferred) application.

  If a user uninstalls a preferred application outside of Citrix Workspace app, the application is unsubscribed during the next Citrix Workspace app refresh. If a user uninstalls a preferred application from the Citrix Workspace app, Citrix Workspace app unsubscribes the application but does not uninstall it.

> **Note:**
>
> The keyword prefer is applied when Citrix Workspace app subscribes an application. Adding the keyword after the application is subscribed has no effect.

You can specify the preferred keyword multiple times for an application. Only one match is needed to apply the keyword to an application. The following patterns can be used in any combination:

- prefer="ApplicationName"

  The application name pattern matches any application with the specified application name in the shortcut file name. The application name can be a word or a phrase. Quotation marks are required for phrases. Matching is not allowed on partial words or file paths and is case-insensitive. The application name matching pattern is useful for overrides performed manually by an administrator.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

KEYWORDS:prefer=	Shortcut under Programs	Matches?
Word	\Microsoft Office\Microsoft Word 2010	Yes
Microsoft Word	\Microsoft Office\Microsoft Word 2010	Yes
Console	McAfee\VirusScan Console	Yes
Virus	McAfee\VirusScan Console	No
Console	McAfee\VirusScan Console	Yes

- prefer="\\Folder1\Folder2\…\ApplicationName"

  The absolute path pattern matches the entire shortcut file path plus the entire application name under the Start menu. The Programs folder is a sub folder of the Start menu directory, so you must include it in the absolute path to target an application in that folder. Quotation marks are required if the path contains spaces. The matching is case-sensitive. The absolute path matching pattern is useful for overrides implemented programmatically in Citrix Virtual Apps and Desktops and Citrix DaaS.

KEYWORDS:prefer=	Shortcut under Programs	Matches?
\Programs\Microsoft Office\Microsoft Word 2010	\Programs\Microsoft Office\Microsoft Word 2010	Yes
\Microsoft Office	\Programs\Microsoft Office\Microsoft Word 2010	No
\Microsoft Word 2010	\Programs\Microsoft Office\Microsoft Word 2010	No
\Programs\Microsoft Word 2010	\Programs\Microsoft Word 2010	Yes

- prefer="\Folder1\Folder2\…\ApplicationName"

  The relative path pattern matches the relative shortcut file path under the Start menu. The relative path provided must contain the application name and can optionally include the folders where the shortcut resides. Matching is successful if the shortcut file path ends with the relative path provided. Quotation marks are required if the path contains spaces. The matching is case-sensitive. The relative path matching pattern is useful for overrides implemented programmatically.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

KEYWORDS:prefer=	Shortcut under Programs	Matches?
\Microsoft Office\Microsoft Word 2010	\Microsoft Office\Microsoft Word 2010	Yes
\Microsoft Office	\Microsoft Office\Microsoft Word 2010	No
\Microsoft Word 2010	\Microsoft Office\Microsoft Word 2010	Yes
\Microsoft Word	\Microsoft Word 2010	No

For information about other keywords, see "Additional recommendations"in Optimize the user experience section in the StoreFront documentation.

Virtual display layout

This feature lets you define a virtual monitor layout that applies to the remote desktop. You can also split a single client monitor virtually into up to eight monitors on the remote desktop. You can configure the virtual monitors in the **Monitor Layout** tab in the Desktop Viewer. There, you can draw horizontal or vertical lines to separate the screen into virtual monitors. The screen is split according to a specified percentage of the client monitor resolution.

You can set a DPI for the virtual monitors that are used for DPI scaling or DPI matching. After applying a virtual monitor layout, resize or reconnect the session.

This configuration applies only to full-screen session, single-monitor desktop sessions, and does not affect any published applications. This configuration applies to all subsequent connections from this client.

Starting from Citrix Workspace app for Windows 2106, virtual display layout is also supported for full-screen and multi-monitor desktop sessions. Virtual display layout is enabled by default. In a multi-monitor scenario, the same virtual display layout is applied to all the session monitors if the total number of virtual displays doesn't exceed eight virtual displays. In case this limit is exceeded, the virtual display layout is ignored and not applied to any session monitor.

Multi-monitor enhancement can be disabled by setting the following registry key:

- `HKEY_CURRENT_USER\Software\Citrix\XenDesktop\DesktopViewer`

Name: **SplitAllMonitors**
Type: DWORD

Values:

1 - Enabled

© 1997–2026 Citrix Systems, Inc. All rights reserved.

0 - Disabled

Application launch time

Use the session prelaunch feature to reduce application launch time during normal or high traffic periods, thus providing users with a better experience. The prelaunch feature allows to create a prelaunch session. Prelaunch session is created when a user logs on to Citrix Workspace app, or at a scheduled time if the user has signed in.

The prelaunch session reduces the launch time of the first application. When a user adds a new account connection to Citrix Workspace app for Windows, session prelaunch doesn't take effect until the next session. The default application ctxprelaunch.exe is running in the session, but it is not visible to you.

For more information, see session prelaunch and session linger guidance in the Citrix Virtual Apps and Desktops article titled Manage delivery groups.

Session prelaunch is disabled by default. To enable session prelaunch, specify the `ENABLEPRELAUNCH=true` parameter on the Workspace command line or set the `EnablePreLaunch` registry key to true. The default setting, null, means that prelaunch is disabled.

> **Note:**
>
> If the client machine has been configured to support Domain Passthrough (SSON) authentication, prelaunch is automatically enabled. If you want to use Domain Pass-through (SSON) without prelaunch, set the **EnablePreLaunch** registry key value to false.

The registry locations are:

- `HKEY_LOCAL_MACHINE\Software\[Wow6432Node\]Citrix\\Dazzle`
- `HKEY_CURRENT_USER\Software\Citrix\Dazzle`

There are two types of prelaunch:

- **Just-in-time prelaunch**- prelaunch starts immediately after the user's credentials are authenticated whether it is a high-traffic period. Typically used for normal traffic periods. A user can trigger just-in-time prelaunch by restarting the Citrix Workspace app.
- **Scheduled prelaunch**- prelaunch starts at a scheduled time. Scheduled prelaunch starts only when the user device is already running and authenticated. If those two conditions are not met when the scheduled prelaunch time arrives, a session does not launch. To share network and server load, the session launches within a window when it is scheduled. For example, if the scheduled prelaunch is scheduled for 13:45, the session actually launches between 13:15 and 13:45. Typically used for high-traffic periods.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Configuring prelaunch on a Citrix Virtual Apps server consists of:

- creating, modifying, or deleting prelaunch applications, and
- updating user policy settings that control the prelaunch application.

You cannot customize the prelaunch feature using the `receiver.admx` file. However, you can change the prelaunch configuration by modifying registry values. Registry values can be modified during or after Citrix Workspace app for Windows installation.

- The HKEY_LOCAL_MACHINE values are written during client installation.
- The HKEY_CURRENT_USER values enable you to provide different users on the same machine with different settings. Users can change the HKEY_CURRENT_USER values without administrative permission. You can provide your users with scripts to change the values.

HKEY_LOCAL_MACHINE registry values:

For 64-bit Windows operating systems: `HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Citrix\ICA Client\Prelaunch`

For 32-bit Windows operating systems: `HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\ICA Client\Prelaunch`

Name: **UserOverride**
Type: REG_DWORD

Values:

0 - Use the HKEY_LOCAL_MACHINE values even if HKEY_CURRENT_USER values are also present.

1 - Use the HKEY_CURRENT_USER values if they exist; otherwise, use the HKEY_LOCAL_MACHINE values.

Name: **State**
Type: REG_DWORD

Values:

0 - Disable prelaunch.

1 - Enable just-in-time prelaunch. (Prelaunch starts after the user's credentials are authenticated.)

2 - Enable scheduled prelaunch. (Prelaunch starts at the time configured for Schedule.)

Name: **Schedule**
Type: REG_DWORD

Value:

The time (24-hour format) and days of a week for the scheduled prelaunch entered in the following format:

© 1997–2026 Citrix Systems, Inc. All rights reserved.

HH:MM	M:T:W:TH:F:S:SU where HH and MM are hours and minutes. M:T:W:TH:F:S:SU is the days of the week. For example, to enable scheduled prelaunch on Monday, Wednesday, and Friday at 13:45, set Schedule as Schedule=13:45	1:0:1:0:1:0:0. The session actually launches between 13:15 and 13:45.

HKEY_CURRENT_USER registry values:

`HKEY_CURRENT_USER\SOFTWARE\Citrix\ICA Client\Prelaunch`

The **State** and **Schedule** keys have the same values as for HKEY_LOCAL_MACHINE.

Bidirectional content redirection

The bidirectional content redirection policy allows you to enable or disable client to host and host to client URL redirection. Server policies are set in Studio, and client policies are set from the Citrix Workspace app Group Policy Object administration template.

Citrix offers host to client redirection and Local App Access for client to URL redirection. However, we recommend that you use bidirectional content redirection for domain-joined Windows clients.

You can enable bidirectional content redirection using one of the following methods:

1. Group Policy Object (GPO) administrative template
2. Registry editor

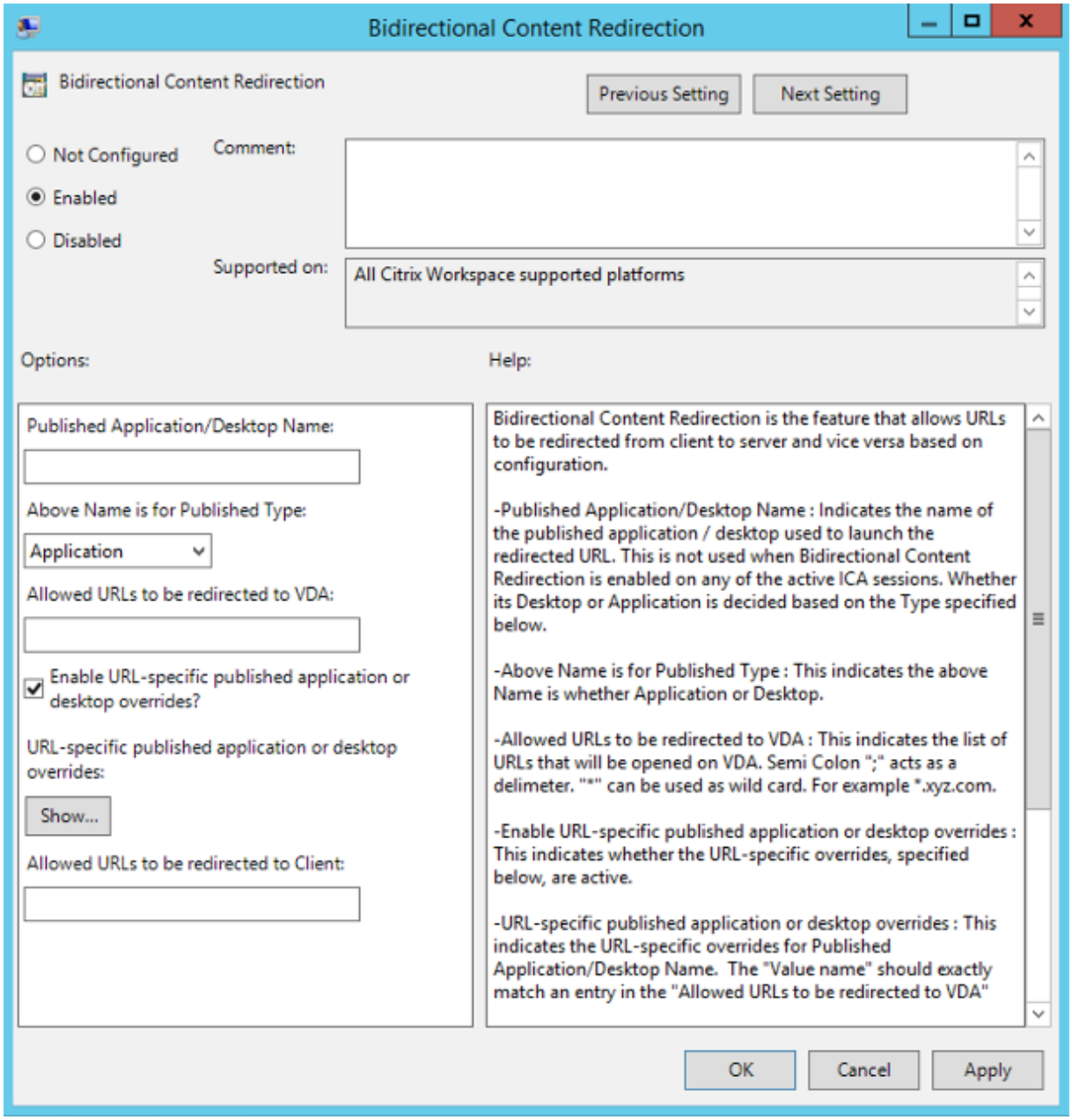
> **Note:**
>
> - Bidirectional content redirection does not work in the session where **Local App Access** is enabled.
> - Bidirectional content redirection must be enabled both on the server and the client. When it is disabled either on the server or the client, the functionality is disabled.
> - When you include URLs, you can specify one URL or a semi-colon delimited list of URLs. You can use an asterisk (*) as a wildcard.

To enable bidirectional content redirection using the GPO administrative template:

Use Group Policy Object administrative template configuration only for a first-time installation of Citrix Workspace app for Windows.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

1. Open the Citrix Workspace app Group Policy Object administrative template by running gpedit.msc.
2. Under the **User Configuration** node, go to **Administrative Templates** > **Classic Administrative Templates (ADM)** > **Citrix Components** > **Citrix Workspace** > **User experience**.
3. Select the **Bidirectional Content Redirection** policy.

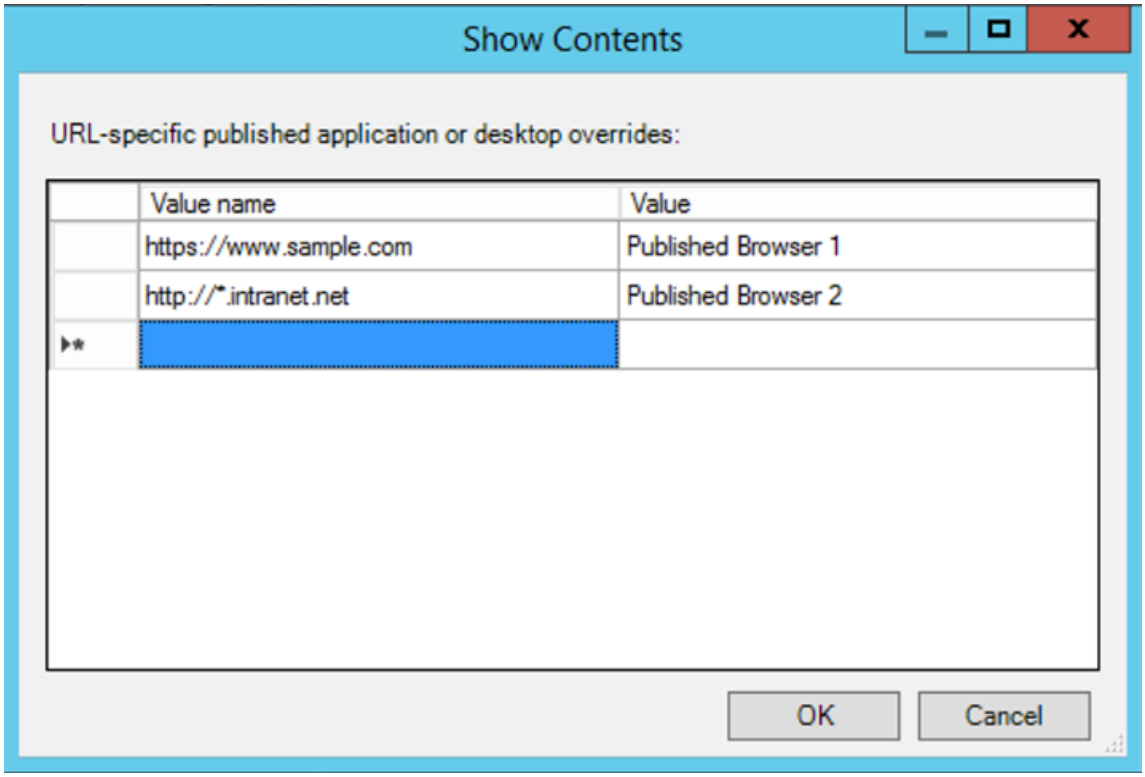


1. In the **Published Application or Desktop name** field, provide the name of the resource used to launch the redirected URL.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

> **Note:**
>
> When you include URLs, specify a single URL or a semi-colon delimited list of URLs. You can use an asterisk (*) as a wildcard.

2. From the **Above Name is for Published Type**, select **Application** or **Desktop** of the resource as appropriate.
3. In the **Allowed URLs to be redirected to VDA** field, enter the URL that must be redirected. Separate the list with a semicolon.
4. Select the **Enable URL-specific published application for desktop overrides?** option to override a URL.
5. Click **Show** to display a list where the value name must match any of the URLs listed in the **Allowed URLs to be redirected to the VDA** field. The value must match a published application name.



6. In the **Allowed URLs to be redirected to Client:** field, enter the URL that must be redirected from the server to the client. Separate the list with a semicolon.

> **Note:**
>
> When you include URLs, specify a single URL or a semi-colon delimited list of URLs. You can use an asterisk (*) as a wildcard.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

7. Click **Apply** and **OK**.
8. From the command line, run the `gpupdate /force` command.

To enable bidirectional content redirection using the registry:

To enable bidirectional content redirection, run the `redirector.exe /RegIE` command from the Citrix Workspace app installation folder `C:\Program Files (x86)\Citrix\ICA Client`).

> **Important:**
>
> - Ensure that the redirection rule does not result in a looping configuration. A looping configuration results if VDA rules are set so that, for example, a URL, `https://www.my\\_company.com` is configured to be redirected to the client, and the VDA.
> - URL redirection supports only explicit URLs: URLs appearing in the address bar of the browser or found using the in-browser navigation, depending on the browser).
> - If two applications with the same display name use multiple StoreFront accounts, the display name in the primary StoreFront account is used for launching the application or a desktop session.
> - A new browser window opens only when a URL is redirected to the client. When a URL is redirected to VDA, if the browser is already open, then the redirected URL opens in the new tab.
> - Embedded links in files like documents, emails, PDF are supported.
> - Ensure that only one of the server file type associations exist and the host content redirection policies are set to Enabled on the same machine. Citrix recommends that you disable either the server file type association or the Host Content (URL) Redirection feature to confirm that URL redirection works properly.

Limitation:

No fallback mechanism is present if the redirection fails due to session launch issues.

Bi-directional URL support with Chromium-based browsers

Bidirectional content redirection allows you to configure URLs to redirect from client to server and from server to client using policies on the server and the client.

Server policies are set on the Delivery Controller and client policies on Citrix Workspace app. The policies are set using the Group Policy Object (GPO) administrative template.

Starting with Version 2106, bidirectional URL redirection support has been added for Google Chrome and Microsoft Edge.

Prerequisites:

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- Citrix Virtual Apps and Desktops Version 2106 or later.
- Browser redirection extension version 5.0.

To register Google Chrome browser to bidirectional URL redirection, run the following command from the Citrix Workspace app installation folder:

```
%ProgramFiles(x86)%\Citrix\ICA Client\redirector.exe /regChrome /
verbose
```

> **Note:**
>
> When using these commands on Chrome browsers, the bidirectional content redirection extension installs automatically from the Chrome Web Store.

To unregister Google Chrome browser from bidirectional URL redirection, run the following command from the Citrix Workspace app installation folder:

```
%ProgramFiles(x86)%\Citrix\ICA Client\redirector.exe /unregChrome /
verbose
```

> **Note:**
>
> If you get the following error when accessing the Browser Extensions page, ignore the message:
>
> ```
> Websocket connection to wss://... failed.
> ```

For information on configuring URL redirection on Citrix Workspace app, see Bidirectional content redirection.

To prevent the desktop viewer window from dimming:

If you have multiple Desktop Viewer windows, by default the desktops that are not active are dimmed. If users want to view multiple desktops simultaneously, information on them might be unreadable. You can disable the default behavior and prevent the **Desktop Viewer** window from dimming by editing the Registry editor.

> **Caution**
>
> Editing the registry incorrectly can cause serious problems that might require you to reinstall your Operating system. Citrix cannot guarantee that problems resulting from the incorrect use of the Registry Editor can be solved. Use the Registry Editor at your own risk. Be sure to back up the registry before you edit it

- On the user device, create a REG_DWORD entry called **DisableDimming** in one of the following keys, depending on whether you want to prevent dimming for the current user of the device or the device itself. An entry exists if the Desktop Viewer has been used on the device:
  - `HKEY_CURRENT_USER\Software\Citrix\XenDesktop\DesktopViewer`

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- HKEY_LOCAL_MACHINE\Software\Citrix\XenDesktop\DesktopViewer

Optionally, instead of controlling dimming, you can define a local policy by creating the same REG_WORD entry in one of the following keys:

- HKEY_CURRENT_USER\Software\Policies\Citrix\XenDesktop\DesktopViewer
- HKEY_LOCAL_MACHINE\Software\Policies\Citrix\XenDesktop\DesktopViewer

Before using these keys, check whether the Citrix Virtual Apps and Desktops and Citrix DaaS administrator has set a policy for this feature.

Set the entry to any non-zero value such as 1 or true.

If no entries are specified or the entry is set to 0, the **Desktop Viewer** window is dimmed. If multiple entries are specified, the following precedence is used. The first entry in this list and its value determine whether the window is dimmed:

1. HKEY_CURRENT_USER\Software\Policies\Citrix\…
2. HKEY_LOCAL_MACHINE\Software\Policies\Citrix\…
3. HKEY_CURRENT_USER\Software\Citrix\…
4. HKEY_LOCAL_MACHINE\Software\Citrix\…

Citrix Casting

The Citrix Ready® workspace hub combines digital and physical environments to deliver apps and data within a secure smart space. The complete system connects devices (or things), like mobile apps and sensors, to create an intelligent and responsive environment.

Citrix Ready workspace hub is built on the Raspberry Pi 3 platform. The device running Citrix Workspace app connects to the Citrix Ready workspace hub and casts the apps or desktops on a larger display. Citrix Casting is supported only on Microsoft Windows 10 Version 1607 and later or Windows Server 2016.

Citrix Casting feature allows instant and secure access of any app from a mobile device and display on a large screen.

> **Note:**
>
> - Citrix Casting for Windows supports Citrix Ready workspace hub Version 2.40.3839 and later. Workspace hub with earlier versions might not get detected or cause a casting error.
> - The Citrix Casting feature is not supported on Citrix Workspace app for Windows (Store).

Prerequisites:

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- Bluetooth enabled on the device for hub discovery.
- Both Citrix Ready workspace hub and Citrix Workspace app must be on the same network.
- Port 55555 is allowed between the device running Citrix Workspace app and the Citrix Ready workspace hub.
- For Citrix Casting, port 1494 must not be blocked.
- Port 55556 is the default port for SSL connections between mobile devices and the Citrix Ready workspace hub. You can configure a different SSL port on the Raspberry Pi's settings page. If the SSL port is blocked, users cannot establish SSL connections to the workspace hub.
- Citrix Casting is supported only on Microsoft Windows 10 Version 1607 and later or Windows Server 2016.

Configure Citrix Casting launch

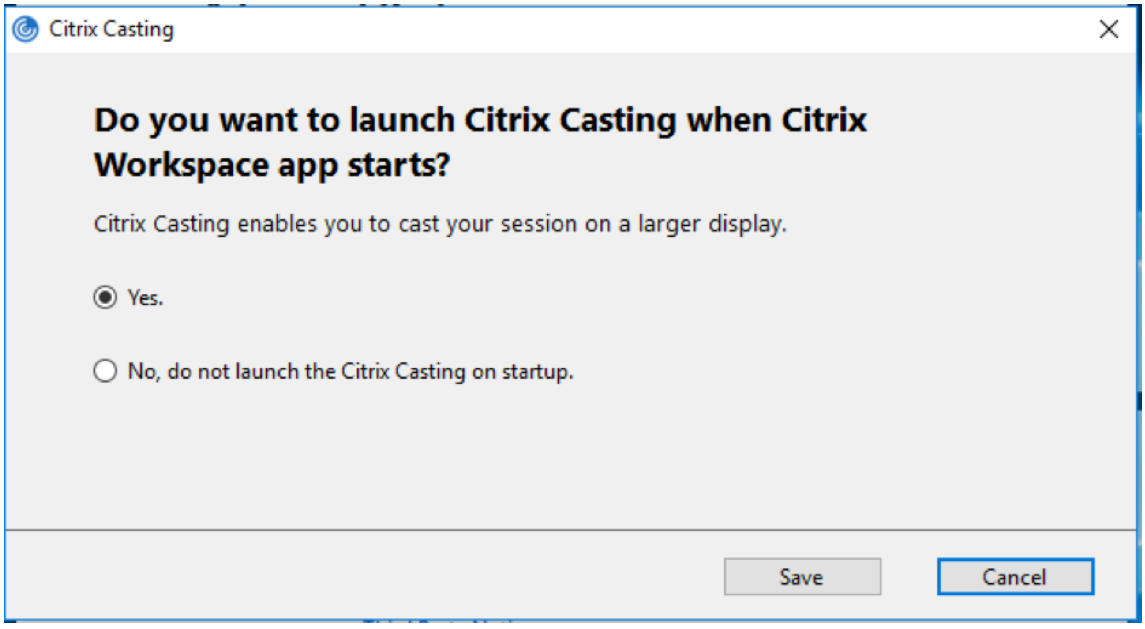
> **Note:**
>
> You can hide all or part of the Advanced Preferences sheet. For more information, see Advanced Preferences sheet.

1. Right-click the Citrix Workspace app icon from the notification area and select **Advanced Preferences**.

   The **Advanced Preferences** dialog appears.

2. Select **Citrix Casting**.

   The **Citrix Casting** dialog appears.



3. Select one of the options:

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- Yes –Indicates that Citrix Casting is launched when Citrix Workspace app starts.
- No, do not launch the Citrix Casting on startup –Indicates that Citrix Casting does not launch when Citrix Workspace app starts.

> **Note:**
>
> Selecting the option **No** does not terminate the current screen casting session. The setting is applied only at the next Citrix Workspace app launch.

4. Click **Save** to apply the changes.

How to use Citrix Casting with Citrix Workspace app

1. Log on to Citrix Workspace app and enable Bluetooth on your device.

   The list of available hubs is displayed. The list is sorted by the RSSI value of the workspace hub beacon package.

2. Select the workspace hub to cast your screen and choose one of the following:

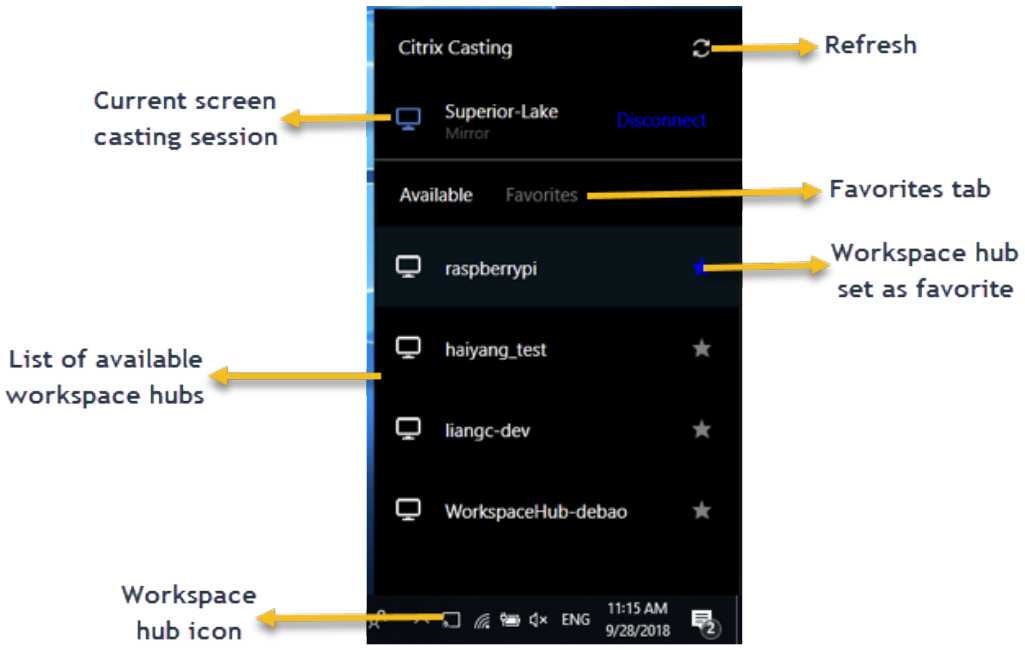
   - **Mirror** to duplicate the primary screen and cast the display to the connected workspace hub device.
   - **Extend** to use the workspace hub device screen as your secondary screen.

> **Note:**
>
> Exiting Citrix Workspace app does not exit Citrix Casting.

In the **Citrix Casting notification** dialog, the following options are available:

1. The current screen casting session displayed at the top.
2. **Refresh** icon.
3. **Disconnect** to stop the current screen casting session.
4. Star icon to add the workspace hub to **Favorites**.
5. Right-click the workspace hub icon in the notification area and select **Exit** to disconnect the screen casting session and to exit Citrix Ready workspace hub.

© 1997–2026 Citrix Systems, Inc. All rights reserved.



Self-check list

If Citrix Workspace app cannot detect and communicate with any available workspace hubs in range, ensure that you do the following as part of self-check:

1. Citrix Workspace app and Citrix Ready workspace hub are connected to the same network.
2. Bluetooth is enabled and working properly on the device where Citrix Workspace app is launched.
3. The device where Citrix Workspace app is launched is within range (less than 10 meters and without any obstructing objects such as walls) of the Citrix Ready workspace hub.
4. Launch a browser in Citrix Workspace app and type `http://<hub_ip>:55555/device-details.xml` to check whether it displays the details of workspace hub device.
5. Click **Refresh** in Citrix Ready workspace hub and try reconnecting to the workspace hub.

Known issues and limitations

1. Citrix Casting does not work unless the device is connected to the same network as the Citrix Ready workspace hub.
2. If there are network issues, there might be a lag in display on the workspace hub device.
3. When you select **Extend**, the primary screen where the Citrix Ready workspace app is launched flashes multiple times.
4. In **Extend** mode, you cannot set the secondary display as the primary display.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

5. The screen casting session automatically disconnects when there is any change in the display settings on the device. For example, change in screen resolution, change in screen orientation.
6. During the screen casting session, if the device running Citrix Workspace app locks, sleeps or hibernates, an error appears at login.
7. Multiple screen casting sessions are not supported.
8. The maximum screen resolution supported by Citrix Casting is 1920 x 1440.
9. Citrix Casting supports Citrix Ready workspace hub Version 2.40.3839 and later. Workspace hub with earlier versions might not get detected or cause a casting error.
10. This feature is not supported on Citrix Workspace app for Windows (Store).
11. On Windows 10, Build 1607, Citrix Casting in **Extend** mode might not be properly positioned.

For more information about the the Citrix Ready workspace hub, see the Citrix Ready workspace hub section in the Citrix Virtual Apps and Desktops documentation.

Composite USB device redirection

USB 2.1 and later supports the notion of USB composite devices where multiple child devices share a single connection with the same USB bus. Such devices employ a single configuration space and shared bus connection where a unique interface number 00-ff is used to identify each child device. Such devices are also not the same as a USB hub which provides a new USB bus origin for other independently addressed USB devices for connection.

Composite devices found on the client endpoint can be forwarded to the virtual host as either:

- a single composite USB device, or
- a set of independent child devices (split devices)

When a composite USB device is forwarded, the entire device becomes unavailable to the endpoint. Forwarding also blocks the local usage of the device for all applications on the endpoint, including the Citrix Workspace client needed for an optimized HDX remote experience.

Consider a USB headset device with both audio device and HID button for mute and volume control. If the entire device is forwarded using a generic USB channel, the device becomes unavailable for redirection over the optimized HDX audio channel. However, you can achieve the best experience when the audio is sent through the optimized HDX audio channel unlike the audio sent using host-side audio drivers through generic USB remoting. The behavior is because of the noisy nature of the USB audio protocols.

You also notice issues when the system keyboard or pointing device are part of a composite device with other integrated features required for the remote session support. When a complete composite device is forwarded, the system keyboard or mouse becomes inoperable at the endpoint, except within the remote desktop session or application.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

To resolve these issues, Citrix recommends that you split the composite device and forward only the child interfaces that use a generic USB channel. Such a mechanism ensures that the other child devices are available for use by applications on the client endpoint, including the Citrix Workspace app that provides optimized HDX experiences, while allowing only the required devices to be forwarded and available to the remote session.

Device Rules:

As with regular USB devices, device rules set in the policy or client Citrix Workspace app configuration on the end point select the composite devices for forwarding. Citrix Workspace app uses these rules to decide which USB devices to allow or prevent from forwarding to the remote session.

Each rule consists of an action keyword (Allow, Connect, or Deny), a colon (**:**), and zero or more filter parameters that match actual devices at the endpoints USB subsystem. These filter parameters correspond to the USB device descriptor metadata used by every USB device to identify itself.

Device rules are clear text with each rule on a single line and an optional comment after a **#** character. Rules are matched top down (descending priority order). The first rule that matches the device or child interface is applied. Subsequent rules that select the same device or interface are ignored.

Sample device rules:

- ALLOW: vid=046D pid=0102 # Allow a specific device by vid/pid
- ALLOW: vid=0505 class=03 subclass=01 # Allow any pid for vendor 0505 when subclass=01
- DENY: vid=0850 pid=040C # Deny a specific device (incl all child devices)
- DENY: class=03 subclass=01 prot=01 # Deny any device that matches all filters
- CONNECT: vid=0911 pid=0C1C # Allow and auto-connect a specific device
- ALLOW: vid=0286 pid=0101 split=01 # Split this device and allow all interfaces
- ALLOW: vid=1050 pid=0407 split=01 intf=00,01 # Split and allow only 2 interfaces
- CONNECT: vid=1050 pid=0407 split=01 intf=02 # Split and auto-connect interface 2
- DENY: vid=1050 pid=0407 split=1 intf=03 # Prevent interface 03 from being remoted

You can use any of the following filter parameters to apply rules to the encountered devices:

Filter parameter	Description
vid=xxxx	USB device vendor ID (four-digit hexadecimal code)
pid=xxxx	USB device product ID (four-digit hexadecimal code)
rel=xxxx	USB device release ID (four-digit hexadecimal code)
class=xx	USB device class code (two-digit hexadecimal code)

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Filter parameter	Description
subclass=xx	USB device subclass code (two-digit hexadecimal code)
prot=xx	USB device protocol code (two-digit hexadecimal code)
split=1 (or split=0)	Select a composite device to be split (or non-split)
intf=xx[,xx,xx,…]	Selects a specific set of child interfaces of a composite device (comma-separated list of two-digit hexadecimal codes)

The first six parameters select the USB devices for which the rule must be applied. If any parameter is not specified, the rule matches a device with ANY value for that parameter.

The USB Implementors Forum maintains a list of defined class, subclass, and protocol values in Defined Class Codes. USB-IF also maintains a list of registered vendor IDs. You can check the vendor, product, release, and interface IDs of a specific device directly in the Windows device manager or using a free tool like UsbTreeView.

When present, the last two parameters apply only to USB composite devices. The split parameter determines if a composite device must be forwarded as split devices or as a single composite device.

- *Split=1* indicates that the selected child interfaces of a composite device must be forwarded as split devices.
- *Split=0* indicates that the composite device must not be split.

> **Note:**
>
> If the split parameter is omitted, *Split=0* is assumed.

The `intf` parameter selects the specific child interfaces of the composite device to which the action must be applied. If omitted, the action applies to all interfaces of the composite device.

Consider a composite USB headset device with three interfaces:

- Interface 0 - Audio class device endpoints
- Interface 3 - HID class device endpoints (volume and mute buttons)
- Interface 5 - Management/update interface

The suggested rules for this type of device are:

- CONNECT: vid=047F pid=C039 split=1 intf=03 # Allow and auto-connect HID device
- DENY: vid=047F pid=C039 split=1 intf=00 # Deny audio end points

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- ALLOW: vid=047F pid=C039 split=1 intf=05 # Allow mgmt `intf` but don't auto-connect

Enable Device Rules policy:

Citrix Workspace app for Windows includes a set of default device rules that filters certain undesirable classes of devices and allow one that customers often encounter.

You can check these default device rules in the system registry at either:

- `HKEY_LOCAL_MACHINE\Software\Citrix\ICA Client\GenericUSB` (32 bit Windows) or
- `HKEY_LOCAL_MACHINE\Software\WOW6432Node\Citrix\ICA Client\GenericUSB` (64 bit Windows), in the multistring value named **DeviceRules**.

However, in the Citrix Workspace app for Window, you can apply **USB Device Rules** policy to overwrite these default rules.

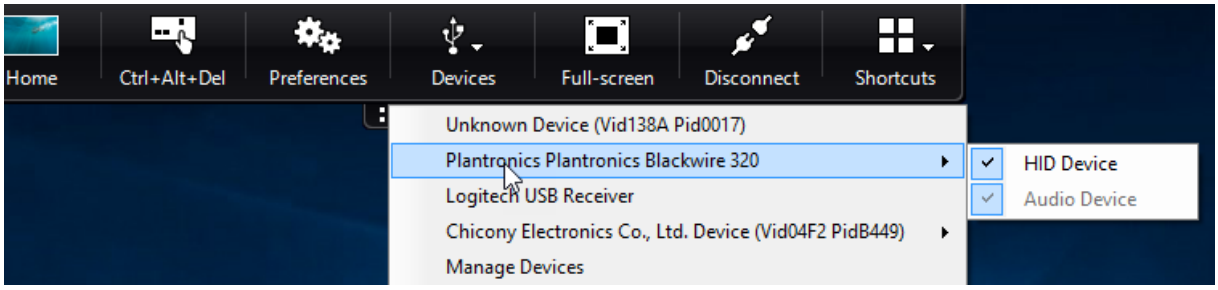
To enable device rules policy for Citrix Workspace app for Windows:

1. Open the Citrix Workspace app Group Policy Object administrative template by running gpedit.msc.
2. Under the **User Configuration** node, go to **Administrative Templates** > **Citrix Components** > **Citrix Workspace** > **Remoting client devices** > **Generic USB Remoting**.
3. Select the **USB Device Rules** policy.
4. Select **Enabled**.
5. In the **USB Device Rules** text box, paste (or edit directly) the USB device rules to be deployed.
6. Click **Apply** and **OK**.

Citrix recommends preserving the default rules shipped with the client when creating this policy by copying the original rules and inserting new rules to alter the behavior as desired.

Connecting USB devices:

In a desktop session, split USB devices are displayed in the Desktop Viewer under **Devices**. Also, you can view split USB devices from **Preferences** > **Devices**.

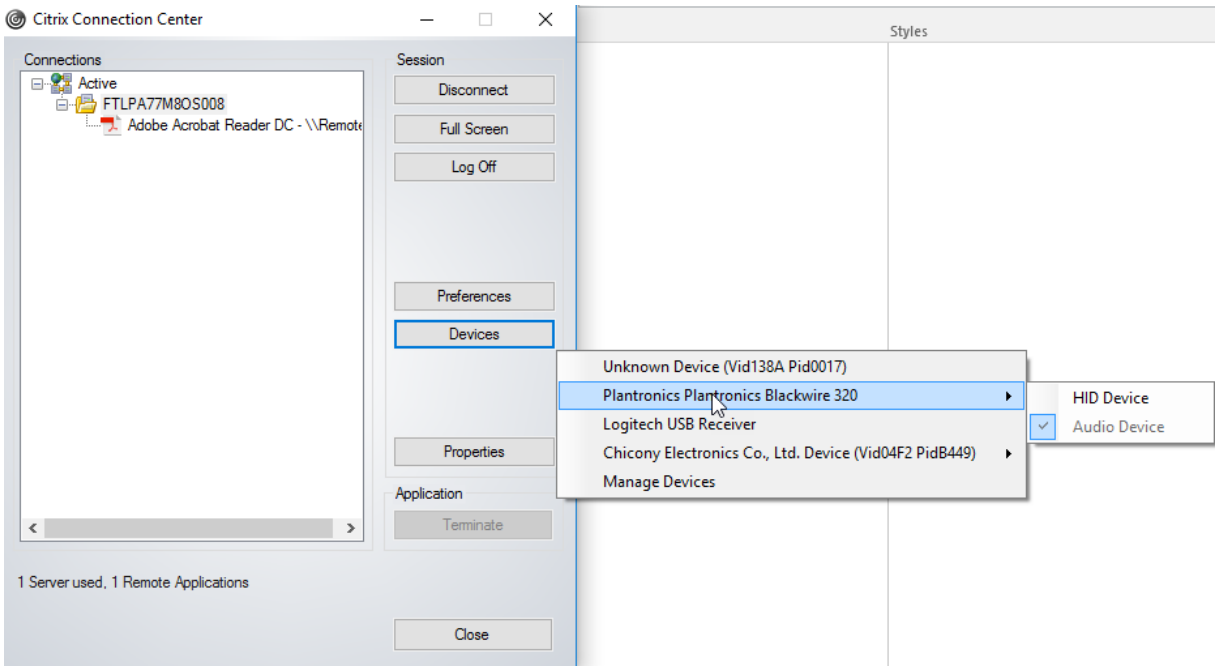


> **Note:**
>
> CONNECT keyword enables automatic connection of a USB device. However, if the CONNECT

© 1997–2026 Citrix Systems, Inc. All rights reserved.

> keyword is not used when you split a composite USB device for generic USB redirection, you must manually select the device from the Desktop Viewer or Connection Center to connect an allowed device.

In an application session, split USB devices are displayed in the **Connection Center**.



To automatically connect an interface:

The CONNECT keyword introduced in Citrix Workspace app for Windows 2109 allows for automatic redirection of USB devices. The CONNECT rule can replace the ALLOW rule if the administrator allows the device or selected interfaces to automatically connect in the session.

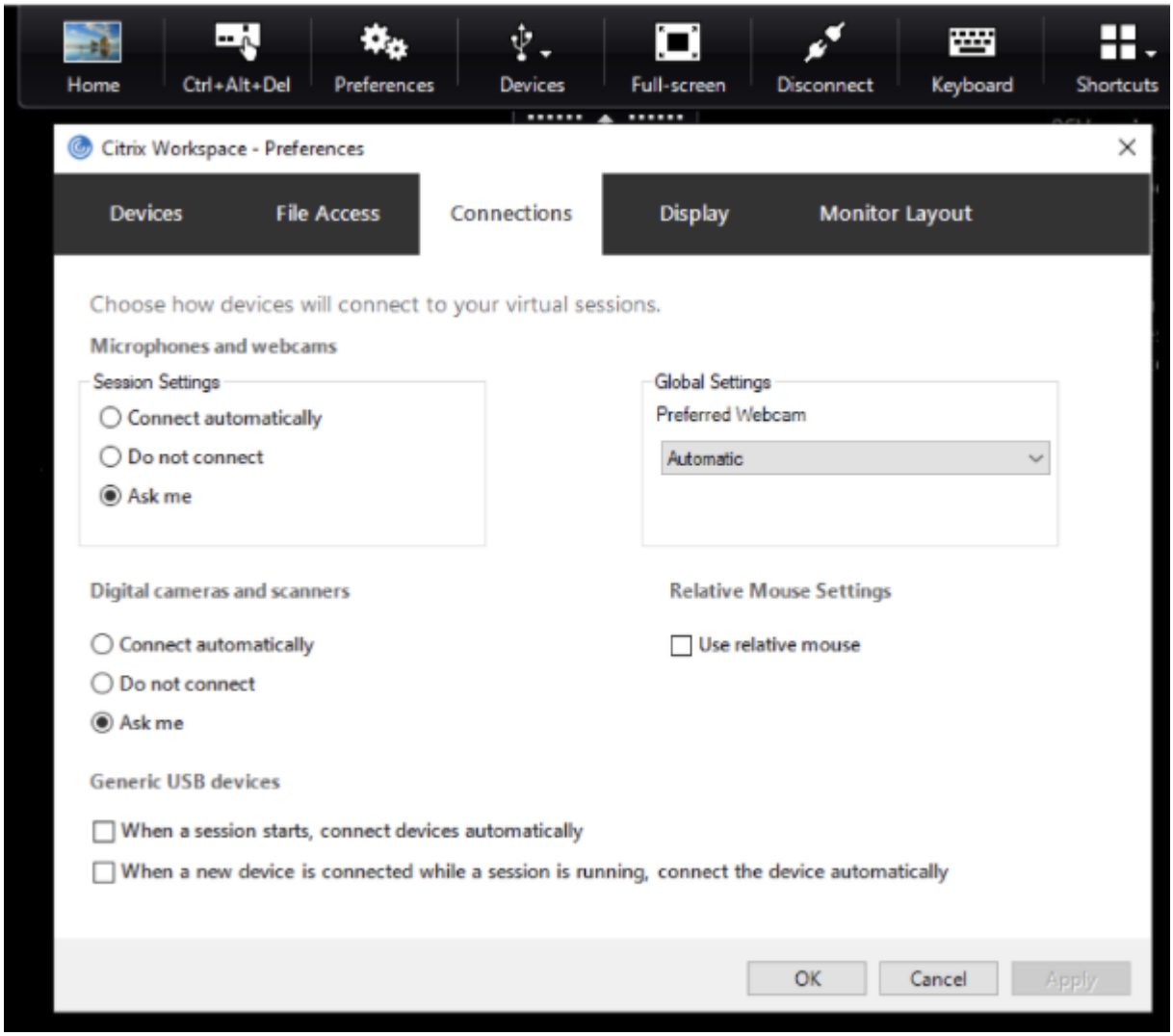
1. Open the Citrix Workspace app Group Policy Object administrative template by running gpedit.msc.
2. Under the **User Configuration** node, go to **Administrative Templates** > **Citrix Components** > **Citrix Workspace** > **Remoting client devices** > **Generic USB Remoting**.
3. Select the **USB Device Rules** policy.
4. Select **Enabled**.
5. In the **USB Device Rules** text box, add the USB device that you want to auto connect.

   For example, `CONNECT: vid=047F pid=C039 split=01 intf=00,03` –allows for splitting a composite device and auto connection of interfaces 00 and 03 interface and restriction other interfaces of that device.
6. Click **Apply** and **OK** to save the policy.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Changing USB device auto-connection preferences:

Citrix Workspace app automatically connects USB devices tagged with CONNECT action based on the preferences set for the current desktop resource. You can change the preferences in the **Desktop viewer** toolbar as shown in the following image.



The two checkboxes at the bottom of the pane controls if the devices must connect automatically or wait for manual connection in the session. These settings are not enabled by default. You can change the preferences if generic USB devices must be connected automatically.

Alternatively, an administrator can override the user preferences by deploying the corresponding policies from the Citrix Workspace app Group Policy Object administrative template. Both machine and user policies can be found under **Administrative Templates** > **Citrix Components** > **Citrix Workspace** > **Remoting client devices** > **Generic USB Remoting**. The corresponding policies are labeled as Existing USB Devices and New USB Devices respectively.

Change split device default setting:

© 1997–2026 Citrix Systems, Inc. All rights reserved.

By default, the Citrix Workspace app for Windows only splits composite devices that are explicitly tagged as *Split=1* in the device rules. However, it is possible to change the default disposition to split all composite devices that are not otherwise tagged with *Split=0* in a matching device rule.

1. Open the Citrix Workspace app Group Policy Object administrative template by running gpedit.msc.
2. Under the **User Configuration** node, go to **Administrative Templates** > **Citrix Components** > **Citrix Workspace** > **Remoting client devices** > **Generic USB Remoting**.
3. Select the **SplitDevices** policy.
4. Select **Enabled**.
5. Click **Apply** and **OK** to save the policy.

> **Note:**
>
> Citrix recommends using explicit device rules to identify specific devices or interfaces that need to be split instead of changing the default. This setting will be deprecated in a future release.

Limitation:

Citrix recommends that you do not split interfaces for a webcam. As a workaround, redirect the device to a single device using Generic USB redirection. For a better performance, use the optimized virtual channel.

Bloomberg keyboards

Citrix Workspace app supports the use of Bloomberg keyboard in a Citrix Virtual Apps and Desktops session. The required components are installed with the plug-in. You can enable the Bloomberg keyboard feature when installing Citrix Workspace app for Windows or by using the Registry editor.

Bloomberg keyboards provide better functionality when compared to standard keyboards that allow the user to access financial market data and perform trades.

The Bloomberg keyboard consists of multiple USB devices built into one physical shell:

- the keyboard
- a fingerprint reader
- an audio device
- a USB hub to connect all of these devices to the system
- HID buttons, for example, Mute, Vol Up, and Vol Down for the audio device

In addition to the normal functionality of these devices, the audio device includes support for some keys, control of the keyboard, and keyboard LEDs.

To use the specialized functionality inside a session, you must redirect the audio device as a USB device. This redirect makes the audio device available to the session, but prevents the audio device from

© 1997–2026 Citrix Systems, Inc. All rights reserved.

being used locally. In addition, the specialized functionality can only be used with one session and cannot be shared between multiple sessions.

Multiple sessions with Bloomberg keyboards are not recommended. The keyboard operates in a single-session environment only.

Configuring Bloomberg keyboard 5:

You must configure various interfaces of the Bloomberg keyboard. From Citrix Workspace Application for Windows 2109, a new CONNECT keyword is introduced to allow automatic connection of USB devices at session startup and device insertion. The CONNECT keyword can be used to replace the ALLOW keyword when the user wants a USB device or interface to connect automatically. The following example uses the CONNECT keyword.

1. Open the Citrix Workspace app Group Policy Object administrative template by running gpedit.msc.
2. Under the **Computer Configuration** node, go to **Administrative Templates** > **Citrix Components** > **Citrix Workspace** > **Remoting client devices** > **Generic USB Remoting**.
3. Select the **SplitDevices** policy.
4. Select **Enabled**.
5. In the **USB Device Rules** text box, add the following rules if it doesn't exist.
    - CONNECT: vid=1188 pid=A101 # Bloomberg 5 Biometric module
    - DENY: vid=1188 pid=A001 split=01 intf=00 # Bloomberg 5 Primary keyboard
    - CONNECT: vid=1188 pid=A001 split=01 intf=01 # Bloomberg 5 Keyboard HID
    - DENY: vid=1188 pid=A301 split=01 intf=02 # Bloomberg 5 Keyboard Audio Channel
    - CONNECT: vid=1188 pid=A301 split=01 intf=00,01 # Bloomberg 5 Keyboard Audio HID

    > **Note:**
    >
    > IIRC, newlines, or semicolon can be used to separate rules which allows to read either single-line or multi-line registry values.

6. Click **Apply** and **OK** to save the policy.
7. In the **Preferences** window, select the **Connections** tab, and select one or both checkboxes to the connect the devices automatically. The **Preferences** window is accessible from the Desktop Toolbar or Connection Manager.

This procedure makes the Bloomberg keyboard 5 ready for use. The DENY rules that are mentioned in the steps enforce the redirection of the primary keyboard and audio channel over an optimized channel but not over Generic USB. The CONNECT rules enable automatic redirection of the fingerprint module, special keys on the keyboard, and keys related to audio control.

Configure Bloomberg keyboard 4 or 3:

© 1997–2026 Citrix Systems, Inc. All rights reserved.

> **Caution**
>
> Editing the registry incorrectly can cause serious problems that might require you to reinstall your operating system. Citrix cannot guarantee that problems resulting from the incorrect use of the Registry editor can be solved. Use the Registry editor at your own risk. Be sure to back up the registry before you edit it.

1. Locate the following keys in the registry:

   `HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\ICA Client\GenericUSB`

2. Do one of the following:

   - To enable this feature, for the entry with type DWORD and Name **EnableBloombergHID**, set the value to 1.
   - To disable this feature, set the value to 0.

Bloomberg keyboard 3 support is available in the online plug-in 11.2 for Windows and subsequent versions.

Bloomberg keyboard 4 support is available for Windows Receiver 4.8 and later versions.

Determining if Bloomberg keyboards support is enabled:

- To check if Bloomberg keyboard support is enabled in the online plug-in, check how the Desktop Viewer reports the Bloomberg keyboard devices. If the Desktop Viewer isn't used, you can check the registry on the machine where the online plug-in is running.
- If support for Bloomberg keyboards is not enabled, the Desktop Viewer shows:
  - two devices for the Bloomberg keyboard 3, that appears as **Bloomberg Fingerprint Scanner** and **Bloomberg Keyboard Audio**.
  - one policy redirected device for Bloomberg keyboard 4. This device appears as **Bloomberg LP Keyboard 2013**.
- If support for Bloomberg keyboards is enabled, there are two devices shown in the Desktop Viewer. One appears as **Bloomberg Fingerprint Scanner** as before, and the other as **Bloomberg Keyboard Features**.
- If the driver for the Bloomberg Fingerprint Scanner device is not installed, the Bloomberg Fingerprint Scanner entry might not appear in the Desktop Viewer. If the entry is missing, the Bloomberg Fingerprint Scanner might not be available for redirection. You can still check the name of the other Bloomberg device where Bloomberg keyboard support is enabled.
- You can also check the value in the registry to know if the support is enabled:
  `HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\ICAClient\GenericUSB\EnableBloombergHID`

© 1997–2026 Citrix Systems, Inc. All rights reserved.

If the value doesn't exist or is 0 (zero), support for Bloomberg keyboards is not enabled. If the value is 1, support is enabled.

Enabling Bloomberg keyboard support:

> **Note:**
>
> Citrix Receiver for Windows 4.8 introduced the support for composite devices through the **Split-Devices** policy. However, you must use the Bloomberg keyboard feature instead of this policy for the Bloomberg keyboard 4.

The support for the Bloomberg keyboard changes the way certain USB devices are redirected to a session. This support is not enabled by default.

- To enable the support during the installation time, specify the value of the **ENABLE_HID_REDIRECTION** property as TRUE at the installation command line. For example:

```
CitrixOnlinePluginFull.exe /silent
ADDLOCAL="ICA_CLIENT,PN_AGENT,SSON,USB"
ENABLE_SSON="no"INSTALLDIR="c:\test"
ENABLE_DYNAMIC_CLIENT_NAME="Yes"
DEFAULT_NDSCONTEXT="Context1,Context2"
SERVER_LOCATION="http://testserver.net"ENABLE_HID_REDIRECTION="
TRUE"
```

- To enable support after installing the online plug-in, edit the Windows Registry on the system where the online plug-in is running:

  1. Open Registry Editor.
  2. Navigate to the following key:
     `HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\ICA Client\GenericUSB`
  3. If the value **EnableBloombergHID** exists, modify it so that the value data is 1.
  4. If the value **EnableBloombergHID** does not exist, create a DWORD value with the name EnableBloombergHID and provide the value data as 1.

Disabling support for the Bloomberg keyboard:

You can disable support for the Bloomberg keyboard in the online plug-in as follows:

1. Open Registry Editor on the system running the online plug-in software.
2. Navigate to the following key:
   `HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\ICA Client\GenericUSB`
3. If the value **EnableBloombergHID** exists, modify it so that the value data is 0 (zero).

   If the value **EnableBloombergHID** doesn't exist, it indicates that the support for the Bloomberg keyboard is not enabled. In such cases, you don't have to modify any registry values.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Using Bloomberg keyboards without enabling support:

- You can use the keyboard without enabling the Bloomberg keyboard support in the online plug-in. However, you cannot have the benefit of sharing the specialized functionality among multiple sessions and you might experience increased network bandwidth from audio.
- Bloomberg keyboard ordinary keys are available in the same way as any other keyboard. You don't have to take any special action.
- To use the specialized Bloomberg keys, you must redirect the Bloomberg keyboard audio device into the session. If you are using the Desktop Viewer, the manufacturer name and device name of the USB devices appears and **Bloomberg Keyboard Audio** appears for the Bloomberg Keyboard audio device.
- To use the fingerprint reader, you must redirect the device to the Bloomberg Fingerprint Scanner. If the drivers for the fingerprint reader are not installed locally, the device only shows:
  - if the online plug-in is set to connect devices automatically or
  - to let the user choose whether to connect devices.

  Also, if the Bloomberg keyboard is connected before establishing the session and the drivers for the fingerprint reader doesn't exist locally, then the fingerprint reader doesn't appear and isn't usable within the session.

> **Note:**
>
> For Bloomberg 3, a single session or the local system can use the fingerprint reader, and cannot be shared. Bloomberg 4 is prohibited for redirection.

Using Bloomberg keyboards after enabling support:

- If you enable support for Bloomberg keyboards in the online plug-in, you have the benefit of sharing the specialized keyboard functionality with multiple sessions. You also experience less network bandwidth from the audio.
- Enabling support for the Bloomberg keyboard prevents the redirection of the Bloomberg Keyboard audio device. Instead, a new device is made available. If you are using the Desktop Viewer, this device is called Bloomberg Keyboard Features. Redirecting this device provides the specialized Bloomberg keys to the session.

Enabling the Bloomberg keyboard support only affects the specialized Bloomberg keys and the audio device. Because the ordinary keys and fingerprint reader are used in the same way as when the support is not enabled.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

DPI scaling

Citrix Workspace app allows the operating system to control the session resolution.

You can apply high DPI in a session but the feature is disabled by default. Session scaling follows the operating system resolution.

You can configure DPI scaling using the following options:

1. Group Policy Object (GPO) administrative template (per machine configuration)
2. Advanced Preferences (per-user configuration)

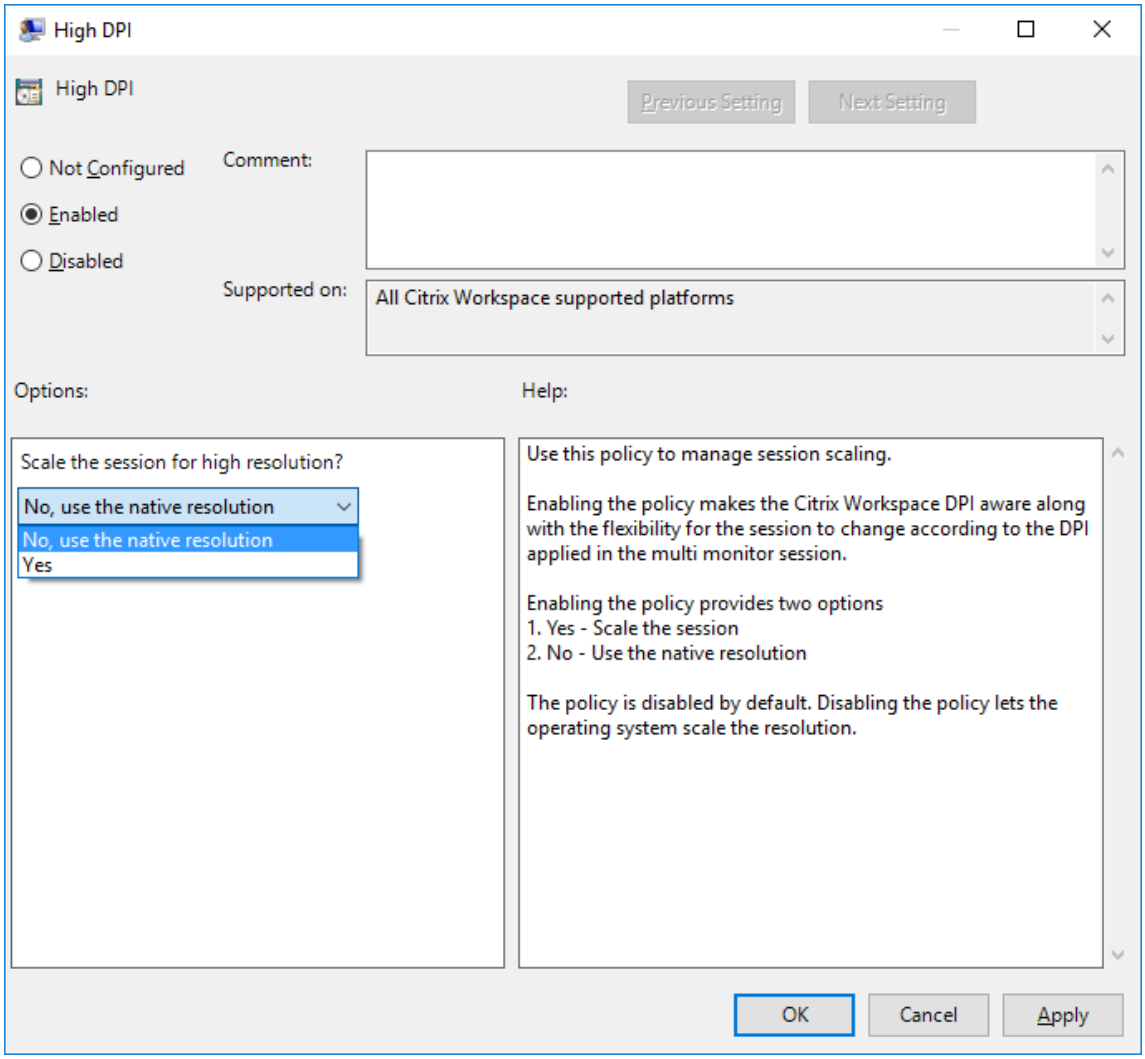
Limitations:

- Even with this feature enabled, a slight blur has been observed in the Desktop Viewer.
- In a session, when you change the DPI settings and relaunch it, the size of the session window might not be appropriate. As a workaround, resize the session window.

To configure DPI scaling using GPO administrative template:

1. Open the Citrix Workspace app Group Policy Object administrative template by running gpedit.msc.
2. Under the **Computer Configuration** node, go to **Administrative Templates**> **Citrix Components** > **Citrix Workspace** > **DPI**
3. Select the **High DPI** policy.

© 1997–2026 Citrix Systems, Inc. All rights reserved.



4. Select from one of the following options:

    a) Yes - Indicates that a high DPI is applied in a session.
    b) No, use the native resolution - Indicates that the resolution is set using the operating system.

5. Click **Apply and OK**.
6. From the command line, run the `gpupdate /force` command to apply the changes.

Configure DPI scaling using the graphical user interface:

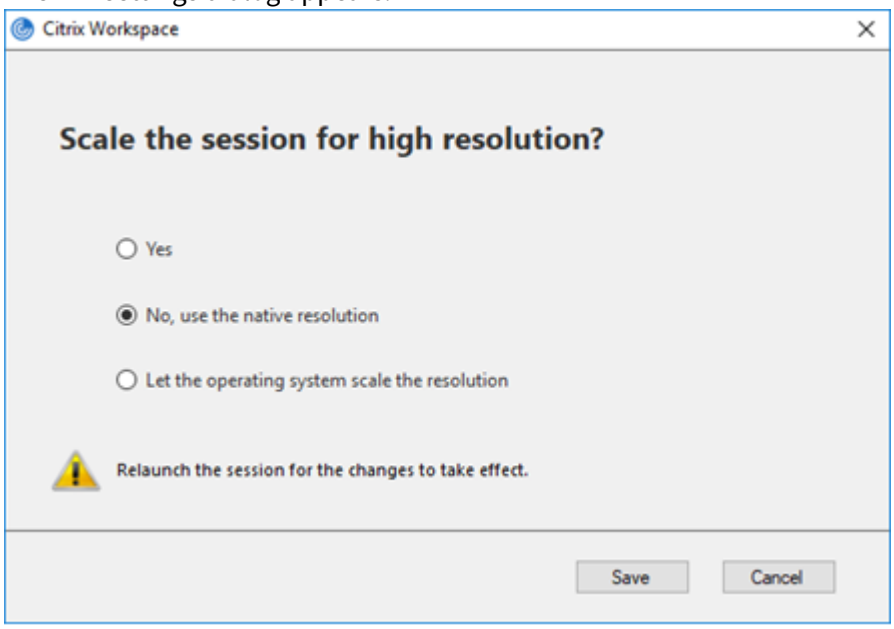
> **Note:**
>
> You can hide all or part of the Advanced Preferences sheet. For more information, see Advanced Preferences sheet.

1. Right-click Citrix Workspace app icon from the notification area.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

2. Select **Advanced Preferences** and click **DPI settings**.

   The DPI settings dialog appears.



3. Select one of the following options:

   a) Yes - Indicates that a high DPI is applied in a session.
   b) No, use the native resolution - Indicates that the Citrix Workspace app detects the DPI on the VDA and applies it.
   c) Let the operating system scale the resolution - By default, this option is selected. It allows the Windows to handle the DPI scaling. This option also means that the High DPI policy is set to disabled.

4. Click **Save**.
5. Restart the Citrix Workspace app session for the changes to take effect.

DPI scaling options

There are three possible settings for DPI scaling in the Citrix Workspace app - Scaled, Unscaled, and Operating system scaling. The use cases for the different settings are as follows.

Scaled:

The scaled setting scales the resolution on the VDA similarly to Operating system scaling, however this setting supports mixed DPI scenarios. The scaled setting corresponds to the UI setting **Yes**, or the High DPI policy set to Enabled in the GPO policy. UI setting **Yes** works well for mixed DPI scenarios when connecting to modern VDAs and allows a way to scale seamless sessions. Scaling might cause

© 1997–2026 Citrix Systems, Inc. All rights reserved.

blurriness in the images, particularly in the case of text. There can be poor performance when connecting to legacy VDAs (6.5, or configured for Legacy Graphics). Local App Access, RTOP, and other plug-ins that use screen positioning APIs might not be compatible with scaling. By design, seamless apps jumps between monitors in this mode to maintain correct scaling.
This setting is recommended for users on Windows 10 connecting to modern VDAs. It supports mixed DPI without any additional impact on server resources.

Unscaled:

The unscaled setting sends the full resolution of all monitors in the session. These resolutions are unscaled and can result in small text and icons in apps and desktops. The unscaled setting corresponds to the UI setting **No** and the HighDPI policy is set to Enabled in the GPO. UI setting **No** doesn't cause any blurriness due to scaling, but can result in small text and icons. When connecting to a desktop session, the DPI can be set within the VDA resulting in the desired scaling. However, such setting is not possible on RDS desktops, or seamless applications. Enabling this setting causes sessions with higher resolution which can impact server performance and scalability.
This setting is recommended for desktop sessions requiring the best image quality, where the additional server resources are acceptable. It can also be used in cases where the small text and icons are not an issue for the user.

Operating system scaling:

Operating system scaling is the default and corresponds to the UI setting **Let the operating system scale the resolution**. The High DPI policy set to Disabled in this scenario. Based on this setting, the Windows Operating system handles the DPI scaling for a session. The resolution on the VDA is scaled based on the DPI, resulting in a smaller resolution than the client device. This works well for single monitor sessions, and is efficient when connecting to 6.5 VDAs, or VDAs configured for Legacy Graphics. This method does not support Mixed DPI- all monitors must have the same DPI or the session does not work. Scaling can cause blurriness in the images, particularly in the case of text. There might also be issues with cursor sizes on the Windows 10 Operating system.
Citrix recommends this setting for users on Windows 7 endpoints, and users connecting to legacy VDAs. It can also be used on Windows 10 if there is no Mixed DPI.

Virtual display layout

This feature lets you define a virtual monitor layout for the remote desktop. You can also split a single client monitor virtually into up to eight monitors on the remote desktop. You can configure the virtual monitors in the **Monitor Layout** tab in the Desktop Viewer. There, you can draw horizontal or vertical lines to separate the screen into virtual monitors. The screen is split according to specified percentage of the client monitor resolution.

You can set a DPI for the virtual monitors that are used for DPI scaling or DPI matching. After applying a virtual monitor layout, resize or reconnect the session.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

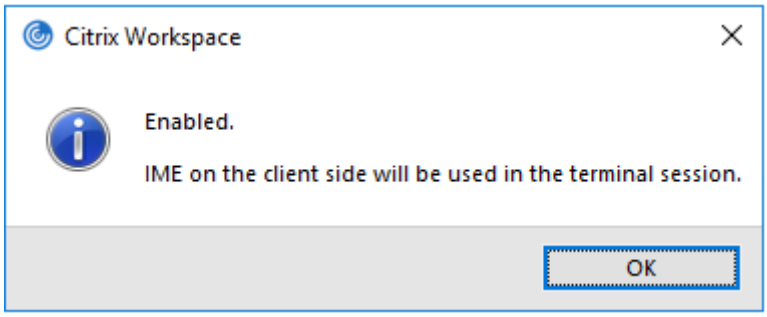
This configuration applies only to full-screen session, single-monitor desktop sessions, and does not affect any published applications. This configuration applies to all subsequent connections from this client.

Generic client Input Method Editors (IME)

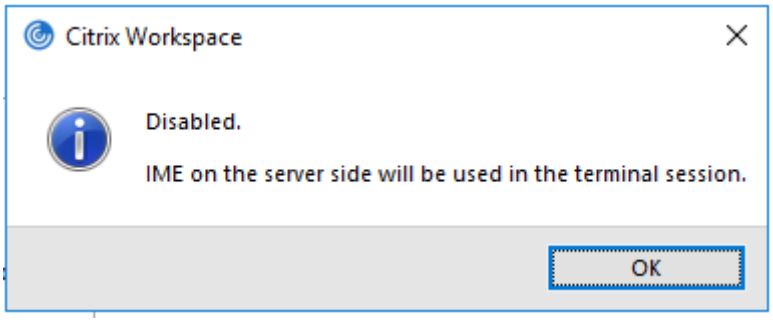
> **Note:**
>
> If you're using a Windows 10 Version 2004 operating system, you might face certain technical issues when using the IME feature in a session. Those issues are the result of a third-party limitation. For more information, see the Microsoft Support article.

Configuring generic client IME using the command-line interface:

- To enable generic client IME, run the `wfica32.exe /localime:on` command from the Citrix Workspace app installation folder `C:\Program Files (x86)\Citrix\ICA Client`.



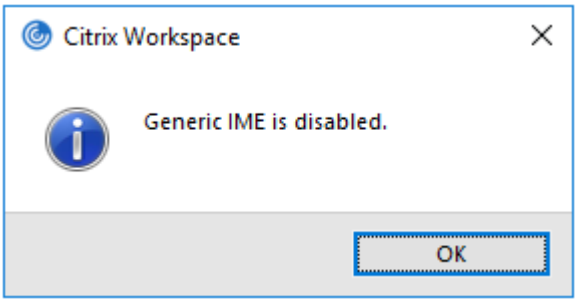
- To disable generic client IME, run the `wfica32.exe /localime:off` command from the Citrix Workspace app installation folder `C:\Program Files (x86)\Citrix\ICA Client`.



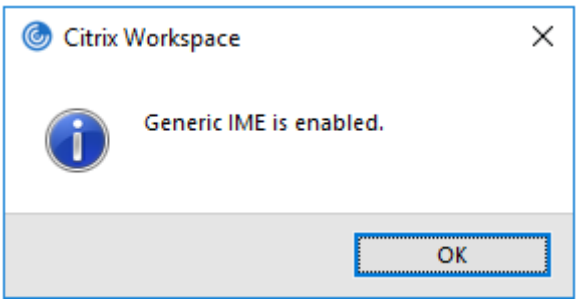
> **Note:**
>
> You can use the command-line switch `wfica32.exe /localime:on` to enable both generic client IME and keyboard layout synchronization.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- To disable generic client IME, run the `wfica32.exe /localgenericime:off` command from the Citrix Workspace app installation folder `C:\Program Files (x86)\Citrix\ICA Client`. This command does not affect the Keyboard Layout Synchronization settings.



If you have disabled generic client IME using the command-line interface, you can enable the feature again by running the `wfica32.exe /localgenericime:on` command.



Toggle:

Citrix Workspace app supports toggle functionality for this feature. You can run the `wfica32.exe /localgenericime:on` command to enable or disable the feature. However, the keyboard layout synchronization settings take precedence over the toggle switch. If keyboard layout synchronization is set to **Off**, toggling does not enable generic client IME.

Configure generic client IME using the graphical user interface:

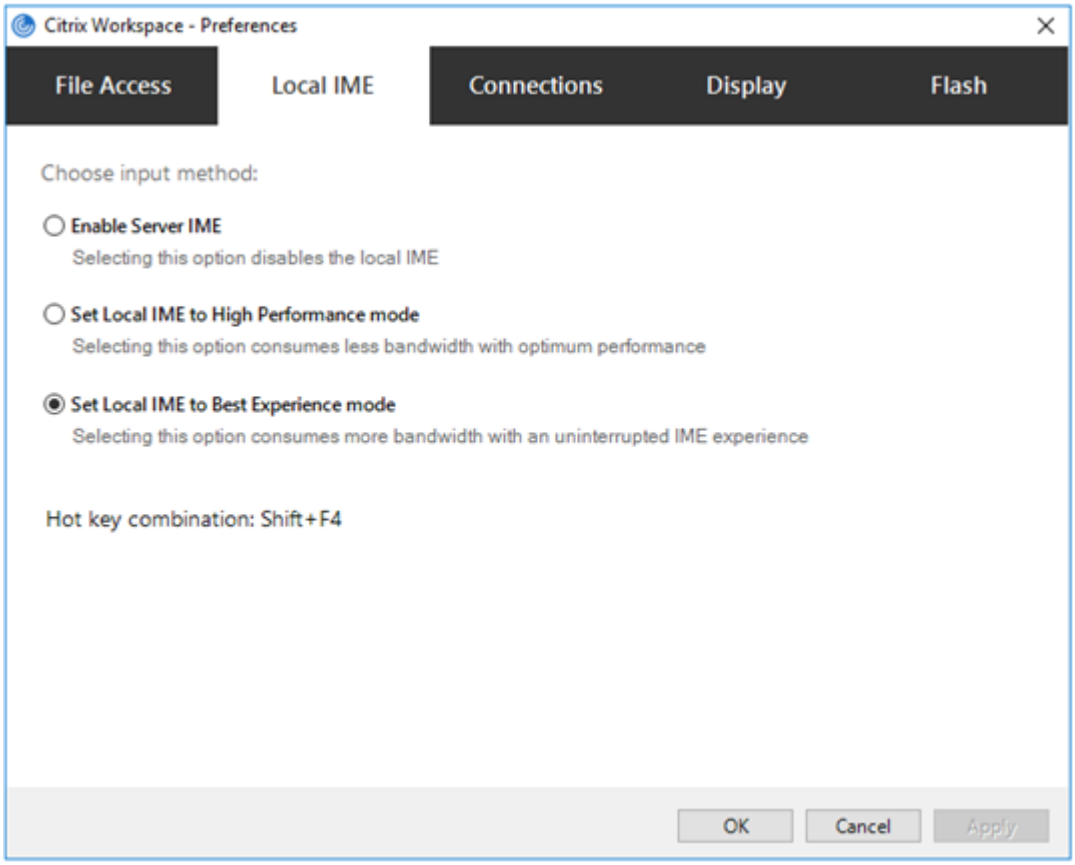
Generic client IME requires VDA Version 7.13 or later.

Generic client IME features can be enabled by enabling keyboard layout synchronization. For more information, see Keyboard layout synchronization.

Citrix Workspace app allows you to configure different options to use generic client IME. You can select from one these options based on your requirements and usage.

1. Right-click the Citrix Workspace app icon in the notification area and select **Connection Center**.
2. Select **Preferences** and **Local IME**.

© 1997–2026 Citrix Systems, Inc. All rights reserved.



The following options are available to support different IME modes:

1. **Enable Server IME** –Disables local IME and only the languages set on the server can be used.
2. **Set Local IME to High Performance mode** –Uses local IME with limited bandwidth. This option restricts the candidate window functionality.
3. **Set Local IME to Best Experience mode** –Uses local IME with best user experience. This option consumes high bandwidth. By default, this option is selected when generic client IME is enabled.

The changes are applied only for the current session.

Enabling hotkey configuration using a registry editor:

When generic client IME is enabled, you can use the **Shift+F4** hotkeys to select different IME modes. The different options for IME modes appear in the top-right corner of the session.

By default, the hotkey for generic client IME is disabled.

In the registry editor, navigate to `HKEY_CURRENT_USER\SOFTWARE\Citrix\ICA Client\Engine\Lockdown Profiles\All Regions\Lockdown\Client Engine\Hot Key`.

Select **AllowHotKey** and change the default value to 1.

You can use the **Shift+F4** hotkeys to select different IME modes in a session.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

The different options for IME modes appear in the top-right corner of the session while switching using these hotkey combinations.



Limitations:

- Generic client IME does not support UWP (Universal Windows Platform) apps such as Search UI, and the Edge browser of the Windows 10 operating system. As a workaround, use the server IME instead.
- Generic client IME is not supported on Internet Explorer Version 11 in **Protected Mode**. As a workaround, you can disable Protected Mode by using **Internet Options**. To disable, click **Security** and clear **Enable Protected Mode**.

H.265 video encoding

Citrix Workspace app supports the use of the H.265 video codec for hardware acceleration of remote graphics and videos. H.265 video codec must be supported and enabled on both the VDA and Citrix Workspace app. If the GPU on the endpoint doesn't support H.265 decoding using the DXVA interface, the H265 Decoding for graphics policy setting is ignored and the session falls back H.264 video codec.

Prerequisites:

1. VDA 7.16 and later.
2. Enable the **Optimize for 3D graphics workload** policy on the VDA.
3. Enable the **Use hardware encoding for video codec** policy on the VDA.

> **Note:**
>
> H.265 encoding is supported only on the NVIDIA GPU.

In Citrix Workspace app for Windows, this feature is set to **Disabled** by default.

Configuring Citrix Workspace app to use H.265 video encoding using Citrix Group Policy Object (GPO) administrative template:

© 1997–2026 Citrix Systems, Inc. All rights reserved.

1. Open the Citrix Workspace app Group Policy Object administrative template by running gpedit.msc.
2. Under the **Computer Configuration** node, go to **Administrative Templates** > **Citrix Workspace** > **User Experience**.
3. Select the **H265 Decoding for graphics** policy.
4. Select **Enabled**.
5. Click **Apply** and **OK**.

Configuring H.265 video encoding using Registry editor:

Enabling H.265 video encoding on a non-domain joined network on a 32-bit operating system:

1. Launch the Registry Editor using regedit on the Run command.
2. Navigate to `HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Citrix\ICA Client\Graphics Engine`.
3. Create a DWORD key by name **EnableH265** and set the value of the key to 1.

Enabling H.265 video encoding on a non-domain joined network on a 64-bit operating system:

1. Launch the Registry Editor using regedit on the Run command.
2. Navigate to `HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Policies\Citrix\ICA Client\Graphics Engine`.
3. Create a DWORD key by the name EnableH265 and set the value of the key to 1.

Restart the session for the changes to take effect.

> **Note:**
>
> - If the **Hardware acceleration for Graphics** policy is disabled in the Citrix Workspace app for Windows Group Policy Object administrative template, the **H265 Decoding for graphics** policy settings are ignored and the feature does not work.
> - Run the HDX Monitor 3.x tool to identify if the H.265 video encoder is enabled within the sessions. For more information about the HDX Monitor 3.x tool, see the Knowledge Center article CTX135817.

Keyboard layout and language bar

Keyboard layout

> **Note:**
>
> You can hide all or part of the Advanced Preferences sheet available from the Citrix Workspace app icon in the notification area. For more information, see Advanced Preferences sheet.

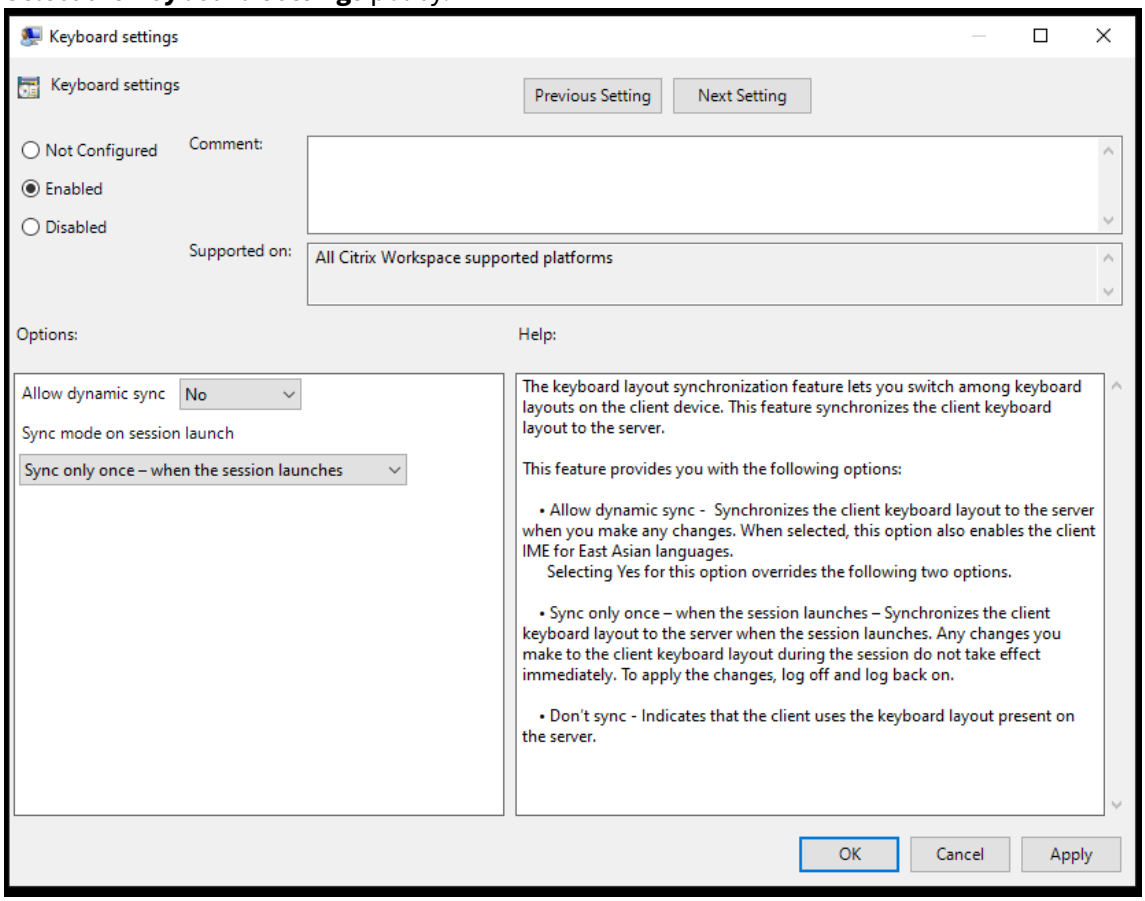
© 1997–2026 Citrix Systems, Inc. All rights reserved.

Keyboard layout synchronization enables you to switch among preferred keyboard layouts on the client device. This feature is disabled by default. The keyboard layout synchronization allows the client keyboard layout to automatically synchronize to the virtual apps and desktops session.

To configure keyboard layout synchronization using the GPO administrative template:

> **Note:**
>
> The GPO configuration takes precedence over the StoreFront and the GUI configurations.

1. Open the Citrix Workspace app Group Policy Object administrative template by running gpedit.msc.
2. Under the **Computer Configuration** or **User Configuration** node, go to **Administrative Templates** > **Administrative Templates (ADM)** > **Citrix Components** > **Citrix Workspace** > **User experience**.
3. Select the **Keyboard settings** policy.



4. Select **Enabled** and select one the following options:

    - **Allow dynamic sync** - From the drop-down menu, select **Yes** or **No**. This option synchronizes the client keyboard layout to the server when you change the client keyboard layout. When selected, this option also enables the client IME for East Asian languages.

      Selecting **Yes** for this option overrides the following two options.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

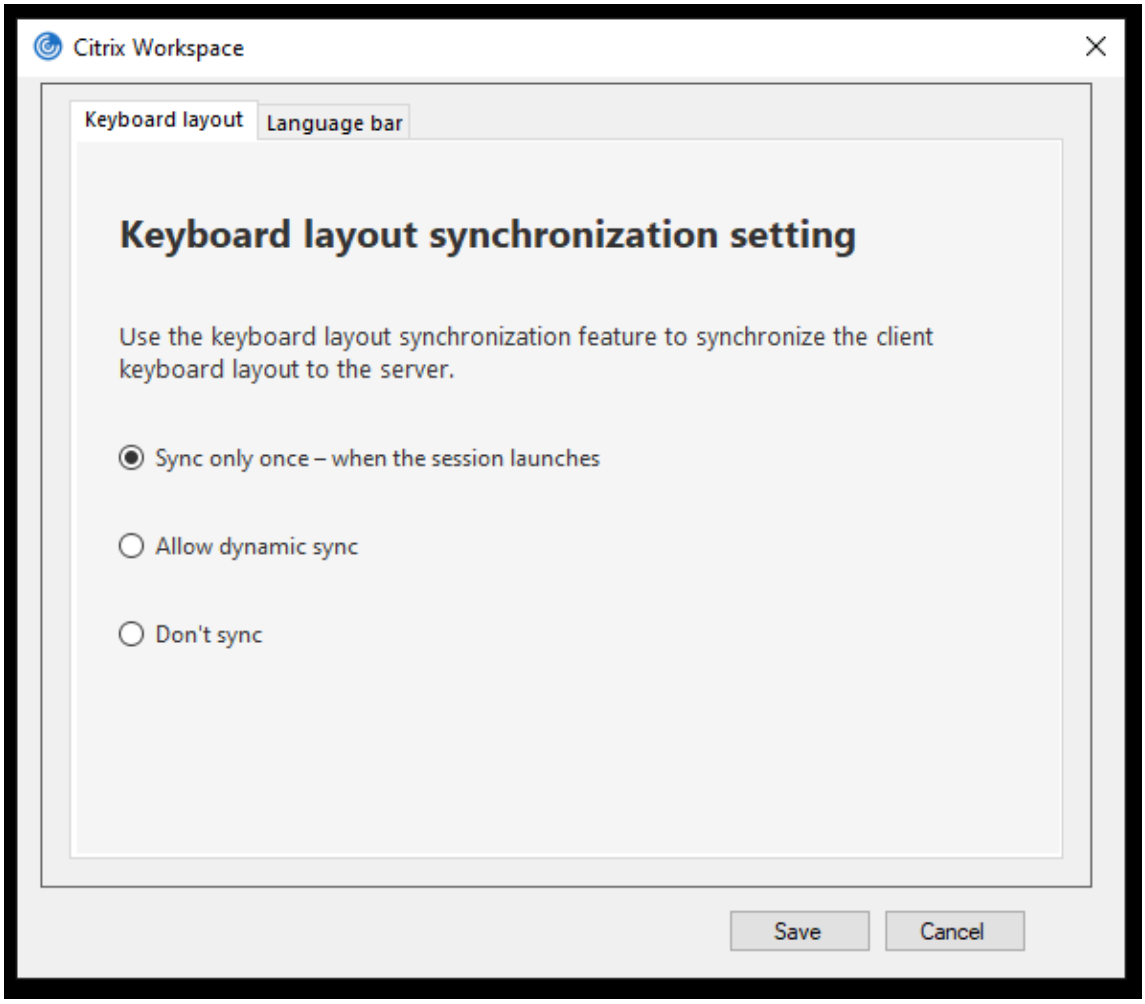
- **Sync mode on session launch** - From the drop-down menu, select one of the following options:
  - **Sync only once - when session launches** - Synchronizes the client keyboard layout to the server when the session launches. Any changes you make to the client keyboard layout during the session do not take effect immediately. To apply the changes, log off and log back on.
  - **Don't sync** - Indicates that the client uses the keyboard layout present on the server.

5. Select **Apply** and **OK**.

To configure keyboard layout synchronization using the graphical user interface:

1. From the Citrix Workspace app icon in the notification area icon, select **Advanced Preferences** > **Keyboard and Language bar**.

   The **Keyboard and Language bar** dialog appears.



2. Select from one of the following options:

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- **Sync only once - when the session launches** - Indicates that the keyboard layout is synced from the VDA only once at the session launch.
- **Allow dynamic sync** - Indicates that the keyboard layout is synced dynamically to the VDA when the client keyboard is changed in a session.
- **Don't sync** - Indicates that the client uses the keyboard layout present on the server.

3. Click **Save**.

To configure keyboard layout synchronization using CLI:

Run the following command from the Citrix Workspace app for Windows installation folder.

Typically, Citrix Workspace app installation folder is at `C:\Program files (x86)\Citrix\ICA Client`.

- To enable: `wfica32:exe /localime:on`
- To disable: `wfica32:exe /localime:off`

Using the client keyboard layout option activates the Client IME (Input Method Editor). If users working in Japanese, Chinese, or Korean prefer to use the Server IME, they must disable the client keyboard layout option by selecting **No**, or running `wfica32:exe /localime:off`. The session reverts to the keyboard layout provided by the remote server when they connect to the next session.

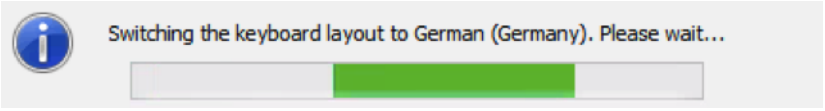
Sometimes, switching the client keyboard layout does not take effect in an active session. To resolve this issue, log off from Citrix Workspace app and login again.

Configuring keyboard sync on Windows VDA

> **Note:**
>
> The following procedure applies only on Windows server 2016 and later. On Windows Server 2012 R2 and earlier, the keyboard sync feature is enabled by default.

1. Launch the Registry editor and navigate to `HKEY_LOCAL_MACHINE\Software\Citrix\IcaIme`.
2. Create the DWORD entry `DisableKeyboardSync` and set its value to `0`.
   1 disables the keyboard layout sync feature.
3. Restart the session for the changes to take effect.

After you enable the keyboard layout on both the VDA and Citrix Workspace app, the following window appears when you switch keyboard layouts.



This window indicates that the session keyboard layout is being switched to the client keyboard layout.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Configuring keyboard sync on Linux VDA

Launch the command prompt and run the following command:

```
/opt/Citrix/VDA/bin/ctxreg update -k "HKEY_LOCAL_MACHINE\System\
    CurrentControlSet\Control\Citrix\LanguageBar" -v "SyncKeyboardLayout
    " -d "0x00000001"
```

Restart the VDA for the changes to take effect.

For more information about the keyboard layout synchronization feature on Linux VDA, see Dynamic keyboard layout synchronization.

Hide the keyboard layout switch notification dialog:

The keyboard layout change notification dialog lets you know that the VDA session is switching the keyboard layout. The keyboard layout switch needs approximately two seconds to switch. When you hide the notification dialog, wait for some time before you start typing to avoid incorrect character input.

> **Warning**
>
> Editing the registry incorrectly can cause serious problems that might require you to reinstall your operating system. Citrix cannot guarantee that problems resulting from the incorrect use of the Registry Editor can be solved. Use the Registry Editor at your own risk. Be sure to back up the registry before you edit it.

Hide the keyboard layout switch notification dialog using the Registry editor:

1. Launch the Registry editor and navigate to `HKEY_LOCAL_MACHINE\Software\Citrix\IcaIme`.
2. Create a String Value key by name **HideNotificationWindow**.
3. Set the DWORD value to **1**.
4. Click **OK**.
5. Restart the session for the changes to take effect.

Limitations:

- Remote applications which run with elevated privilege (for example, right-click an application icon > Run as administrator) cannot be synchronized with the client keyboard layout. As a workaround, manually change the keyboard layout on the server side (VDA) or disable UAC.
- If the user changes the keyboard layout on the client to a layout that isn't supported on the server, the synchronization feature of the keyboard layout is disabled for security reasons. An unrecognized keyboard layout is treated as a potential security threat. To restore the keyboard layout synchronization feature, log off and relog in to the session.
- In an RDP session, you cannot change the keyboard layout using `Alt + Shift` shortcuts. As a workaround, use the language bar in the RDP session to switch the keyboard layout.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Language bar

The language bar displays the preferred input language in a session. The language bar appears in a session by default.

> **Note:**
>
> This feature is available in sessions running on VDA 7.17 and later.

Configure the language bar using the GPO administrative template:

The language bar displays the preferred input language in an application session.

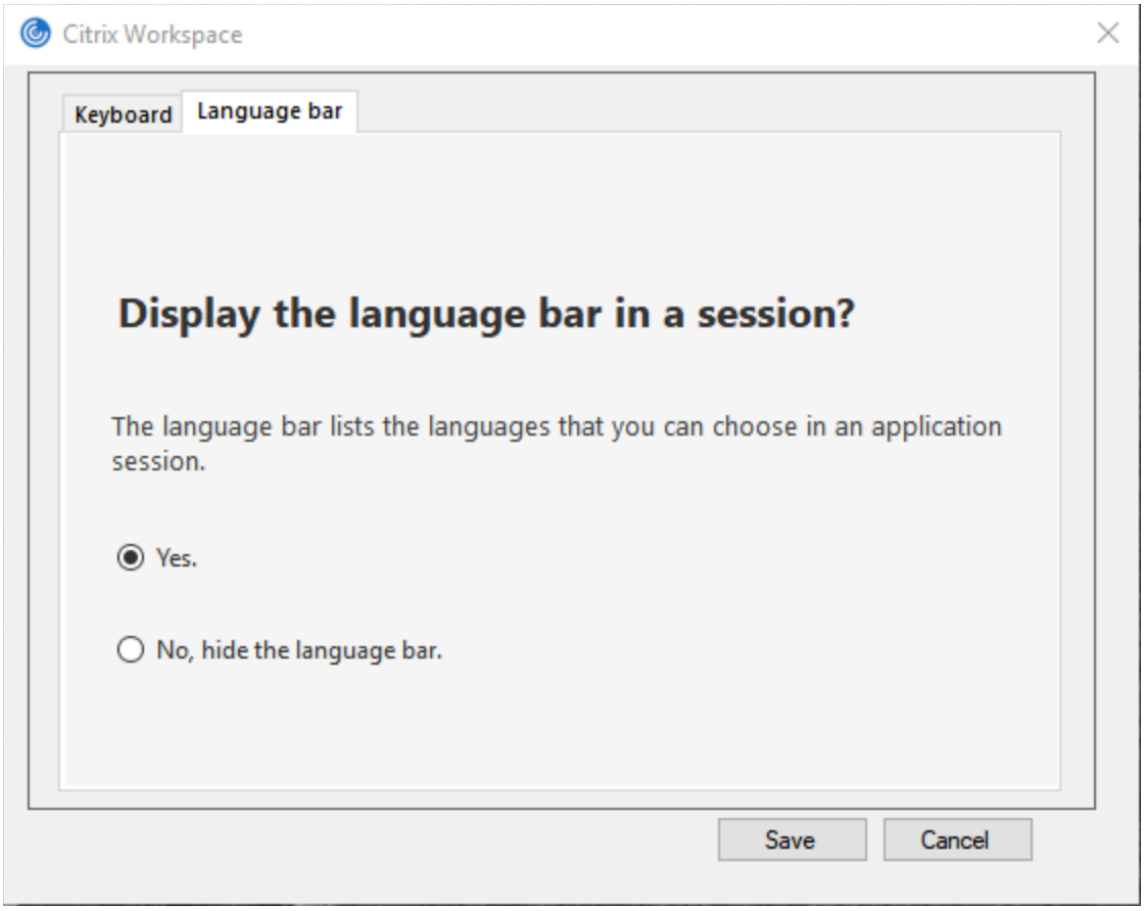
1. Open the Citrix Workspace app Group Policy Object administrative template by running gpedit.msc.
2. Under the **Computer Configuration** or **User Configuration** node, go to **Administrative Templates** > **Administrative Templates (ADM)** > **Citrix Components** > **Citrix Workspace** > **User experience**.
3. Select the **Language bar** policy.
4. Select **Enabled** and select one of the following options:
   - Yes –Indicates that the language bar is displayed in an application session.
   - No, hide the language bar –Indicates that the language bar is hidden in an application session.
5. Click **Apply** and **OK**.

Configure language bar using the graphical user interface:

1. Right-click the Citrix Workspace app icon from the notification area and select **Advanced Preferences**.
2. Select **Keyboard and Language bar**.
3. Select the **Language bar** tab.
4. Select from one of the following options:
   a) Yes - Indicates that the language bar is displayed in a session.
   b) No, hide the language bar - Indicates that the language bar is hidden in a session.
5. Click **Save**.

   The setting changes take effect immediately.

© 1997–2026 Citrix Systems, Inc. All rights reserved.



> **Note:**
>
> - You can change the settings in an active session.
> - The remote language bar does not appear in a session if there is only one input language.

Hide the language bar tab from the Advanced Preferences sheet:

You can hide the language bar tab from the **Advanced Preferences** sheet by using the registry.

1. Launch the registry editor.
2. Navigate to `HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\ICA Client\Engine\Configuration\Advanced\Modules\LocalIME`.
3. Create a DWORD value key, **ToggleOffLanguageBarFeature**, and set it to **1** to hide the Language bar option from the Advanced Preferences sheet.

USB support

USB support enables you to interact with a wide range of USB devices when connected to a Citrix Virtual Apps and Desktops and Citrix DaaS. You can plug USB devices into their computers and the

© 1997–2026 Citrix Systems, Inc. All rights reserved.

devices are remote to their virtual desktop. USB devices available for remoting include flash drives, smartphones, PDAs, printers, scanners, MP3 players, security devices, and tablets. Desktop Viewer users can control whether USB devices are available on the Citrix Virtual Apps and Desktops and Citrix DaaS using a preference in the toolbar.

Isochronous features in USB devices, such as webcams, microphones, speakers, and headsets are supported in typical low latency or high-speed LAN environments. Such environment allows these devices to interact with packages, like Microsoft Office Communicator and Skype.

The following types of device are supported directly in a virtual apps and desktops session, and so does not use USB support:

- Keyboards
- Mice
- Smart cards

Specialist USB devices (for example, Bloomberg keyboards and 3-D mice) can be configured to use USB support. For information on configuring Bloomberg keyboards, see Configure Bloomberg keyboards.

For information on configuring policy rules for other specialist USB devices, see Knowledge Center article CTX122615.

By default, certain types of USB devices are not supported for remoting through Citrix Virtual Apps and Desktops and Citrix DaaS. For example, a user might have a NIC attached to the system board by internal USB. Remoting this device would not be appropriate. The following types of USB device are not supported by default in a virtual apps and desktops session:

- Bluetooth dongles
- Integrated NIC
- USB hubs
- USB graphics adapters

USB devices connected to a hub can be remote, but the hub itself cannot be remote.

The following types of USB device are not supported by default for use in a virtual apps session:

- Bluetooth dongles
- Integrated NIC
- USB hubs
- USB graphics adapters
- Audio devices
- Mass storage devices

How USB support works:

© 1997–2026 Citrix Systems, Inc. All rights reserved.

When a user plugs in a USB device, it is checked against the USB policy, and, if allowed, remoted to the virtual desktop. If the default policy denies a device, it is available only to the local desktop.

When a user plugs in a USB device, a notification appears to inform the user about a new device. The user can select which USB devices must be remoted to the virtual desktop each time they connect. Alternatively, the user can configure USB support so that all USB devices plugged in both before and/or during a session is automatically remoted to the virtual desktop that is in focus.

Mass storage devices

For mass storage devices only, in addition to USB support, remote access is available through client drive mapping. You can configure this through the Citrix Workspace app for Windows policy **Remoting client devices** > **Client drive mapping**. When you apply this policy, the drives on the user device automatically map to drive letters on the virtual desktop when users log on. The drives are displayed as shared folders with mapped drive letters.

The main differences between the two types of remoting policy are:

Feature	Client drive mapping	USB support
Enabled by default	Yes	No
Read-only access configurable	Yes	No
Safe to remove device during a session	No	Yes, if the user clicks Safely Remove Hardware in the notification area

If you enable both Generic USB and the client drive-mapping policies and insert a mass storage device before a session starts, it is redirected using client drive mapping first, before being considered for redirection through USB support. If it is inserted after a session has started, it will be considered for redirection using USB support before client drive mapping.

USB device classes allowed by default:

Default USB policy rules allow different classes of USB device.

Although they are on this list, some classes are only available for remoting in virtual apps and desktops sessions after additional configuration. Such USB device classes are as follows.

- **Audio (Class 01)**- Includes audio input devices (microphones), audio output devices, and MIDI controllers. Modern audio devices generally use isochronous transfers that XenDesktop® 4 or later supports. Audio (Class01) is not applicable to Citrix Virtual Apps because these devices are not available for remoting in Citrix Virtual Apps using USB support.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

> **Note:**
>
> Some specialty devices (for example, VOIP phones) require additional configuration.

- **Physical Interface Devices (Class 05)**- These devices are similar to Human Interface Devices (HIDs), but generally provide "real-time"input or feedback and include force feedback joysticks, motion platforms, and force feedback endoskeletons.
- **Still Imaging (Class 06)**- Includes digital cameras and scanners. Digital cameras often support the still imaging class which uses the Picture Transfer Protocol (PTP) or Media Transfer Protocol (MTP) to transfer images to a computer or other peripheral. Cameras might also appear as mass storage devices. It might be also possible to configure a camera to use either class, through the setup menus provided by the camera itself.

> **Note:**
>
> If a camera appears as a mass storage device, client drive mapping is used and USB support is not required.

- **Printers (Class 07)**- In general most printers are included in this class, although some use vendor-specific protocols (class ff). Multi-function printers might have an internal hub or be composite devices. In both cases the printing element generally uses the Printers class and the scanning or fax element uses another class; for example, Still Imaging.

  Printers normally work appropriately without USB support.

  > **Note**
  >
  > This class of device (in particular printers with scanning functions) requires additional configuration.

- **Mass Storage (Class 08)**- The most common mass storage devices are USB flash drives; others include USB-attached hard drives, CD/DVD drives, and SD/MMC card readers. There are a wide variety of devices with internal storage that also present a mass storage interface; these include media players, digital cameras, and mobile phones. Mass Storage (Class 08) is not applicable to Citrix Virtual Apps because these devices are not available for remoting in Citrix Virtual Apps using USB support. Known subclasses include:

  - 01 Limited flash devices
  - 02 Typically CD/DVD devices (ATAPI/MMC-2)
  - 03 Typically tape devices (QIC-157)
  - 04 Typically floppy disk drives (UFI)
  - 05 Typically floppy disk drives (SFF-8070i)
  - 06 Most mass storage devices use this variant of SCSI

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Mass storage devices can often be accessed through client drive mapping, and so USB support is not required.

- **Content Security (Class 0d)**- Content security devices enforce content protection, typically for licensing or digital rights management. This class includes dongles.
- **Video (Class 0e)**- The video class cover devices that are used to manipulate video or video-related material. Devices, such as webcams, digital camcorders, analog video converters, some television tuners, and some digital cameras that support video streaming.

> **Important**
>
> Most video streaming devices use isochronous transfers that XenDesktop 4 or later supports. Some video devices (for example webcams with motion detection) require additional configuration.

- **Personal Healthcare (Class 0f)**- These devices include personal healthcare devices such as blood pressure sensors, heart rate monitors, pedometers, pill monitors, and spirometry.
- **Application and Vendor Specific (Classes fe and ff)**- Many devices use vendor-specific protocols or protocols not standardized by the USB consortium, and such devices usually appear as vendor-specific (class ff).

USB devices classes denied by default

Default USB policy rules don't allow the following different classes of USB device:

- Communications and CDC Control (Classes 02 and 0a). The default USB policy doesn't allow these devices, because one of the devices might be providing the connection to the virtual desktop itself.
- Human Interface Devices (Class 03). Includes a wide variety of both input and output devices. Typical Human Interface Devices (HIDs) are keyboards, mice, pointing devices, graphic tablets, sensors, game controllers, buttons, and control functions.

  Subclass 01 is known as the "boot interface"class and is used for keyboards and mice.

  The default USB policy doesn't allow USB keyboards (class 03, subclass 01, protocol 1), or USB mice (class 03, subclass 01, protocol 2). The reason is most keyboards and mice are handled appropriately without USB support. Also, it is normally necessary to use these devices locally as well remotely when you connect to a virtual desktop.
- USB Hubs (Class 09). USB hubs allow extra devices to be connected to the local computer. It is not necessary to access these devices remotely.
- Smart Card (Class 0b). Smart card readers include contactless and contact smart card readers, and also USB tokens with an embedded smart card-equivalent chip.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Smart card readers are accessed using smart card remoting and do not require USB support.

- Wireless Controller (Class e0). Some of these devices might be providing critical network access, or connecting critical peripherals, such as Bluetooth keyboards or mice.

  The default USB policy does not allow these devices. However, there might be particular devices to which it is appropriate to provide access using USB support.

- **Miscellaneous network devices (Class ef, subclass 04)**- Some of these devices might be providing critical network access. The default USB policy does not allow these devices. However, there might be particular devices to which it is appropriate to provide access using USB support.

Update the list of USB devices available for remoting

Edit the Citrix Workspace for Windows template file to update the range of USB devices available for remoting to desktops. The update allows you to make changes to Citrix Workspace app for Windows using Group Policy. The file is in the following installed folder:

`\C:\Program Files\Citrix\ICA Client\Configuration\en`

Alternatively, you can edit the registry on each user device, adding the following registry key:

HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Citrix\ICA Client\GenericUSB Type=String Name=”DeviceRules”Value=

> **Important**
>
> Editing the Registry incorrectly can cause serious problems that might require you to reinstall your operating system. Citrix cannot guarantee that problems resulting from the incorrect use of the Registry Editor can be solved. Use the Registry Editor at your own risk. Be sure to back up the registry before you edit it.

The product default rules are stored in:

HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\ICA Client\GenericUSB Type=MultiSz Name=”DeviceRules”Value=

Do not edit the product default rules.

For more information about USB devices policy settings, see USB devices policy settings in Citrix Virtual Apps and Desktops documentation.

Configuring USB audio

> **Note:**
>
> - When you upgrade or install Citrix Workspace app for Windows for the first time, add the

© 1997–2026 Citrix Systems, Inc. All rights reserved.

> latest template files to the local GPO. For more information on adding template files to the local GPO, see Group Policy Object administrative template. For upgrade, the existing settings are retained while importing the latest files.
> - This feature is available only on Citrix Virtual Apps server.

To configure USB audio devices:

1. Open the Citrix Workspace app Group Policy Object administrative template by running gpedit.msc.
2. Under the **Computer Configuration** node, go to **Administrative Templates > Classic Administrative Templates (ADM) > Citrix Components > Citrix Workspace > User experience**, and select **Audio through Generic USB Redirection**.
3. Edit the settings.
4. Click **Apply** and **OK**.
5. Open the cmd prompt in administrator mode.
6. Run the following command
   `gpupdate /force`.

vPrefer launch

In earlier releases, you can specify that the instance of an app installed on the VDA (referred to as local instance in this document) must be launched in preference to the published application by setting the KEYWORDS:prefer=”application”attribute in **Citrix Studio**.

Starting with Version 4.11, in a double-hop scenario (where Citrix Workspace app is running on the VDA that hosts your session), you can now control whether Citrix Workspace app launches:

- the local instance of an application installed on the VDA (if available as a local app) or
- a hosted instance of the application.

vPrefer is available on StoreFront Version 3.14 and Citrix Virtual Desktops 7.17 and later.

When you launch the application, Citrix Workspace app reads the resource data present on the StoreFront server and applies the settings based on the **vprefer** flag at the time of enumeration. Citrix Workspace app searches for the application’s installation path in the Windows registry of the VDA. If present, launches the local instance of the application. Otherwise, a hosted instance of the application is launched.
If you launch an application that is not on the VDA, Citrix Workspace app launches the hosted application. For more information on how StoreFront handled the local launch, see Control of local application launch on published desktops in the Citrix Virtual Apps and Desktops documentation.

If you do not want the local instance of the application to be launched on the VDA, set the **LocalLaunchDisabled** to **True** using the PowerShell on the Delivery Controller. For more information, see the Citrix Virtual Apps and Desktops documentation.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

This feature helps to launch applications faster, thereby providing a better user experience. You can configure it by using the Group Policy Object (GPO) administrative template. By default, vPrefer is enabled only in a double-hop scenario.

> **Note:**
>
> When you upgrade or install Citrix Workspace app for the first time, add the latest template files to the local GPO. For more information on adding template files to the local GPO, see Group Policy Object administrative template. For an upgrade, the existing settings are retained while importing the latest files.

1. Open the Citrix Workspace app GPO administrative template by running gpedit.msc.
2. Under the **Computer Configuration** node, go to **Administrative Template** > **Citrix Component** > **Citrix Workspace** > **SelfService**.
3. Select the **vPrefer** policy.
4. Select **Enabled**.
5. From the **Allow apps** drop-down list, select one of the following options:
    - **Allow all apps**: This option launches the local instance of all apps on the VDA. Citrix Workspace app searches for the installed application, including the native Windows apps such as Notepad, Calculator, WordPad, Command prompt. It then launches the application on the VDA instead of the hosted app.
    - **Allow installed apps**: This option launches the local instance of the installed app on the VDA. If the app is not installed on the VDA, it launches the hosted app. By default, **Allow installed apps** is selected when the **vPrefer** policy is set to **Enabled**. This option excludes the native Windows operating system applications like Notepad, Calculator.
    - **Allow network apps**: This option launches the instance of an app that is published on a shared network.
6. Click **Apply** and **OK**.
7. Restart the session for the changes to take effect.

Limitation:

- Workspace for web does not support this feature.

StoreFront Cloud

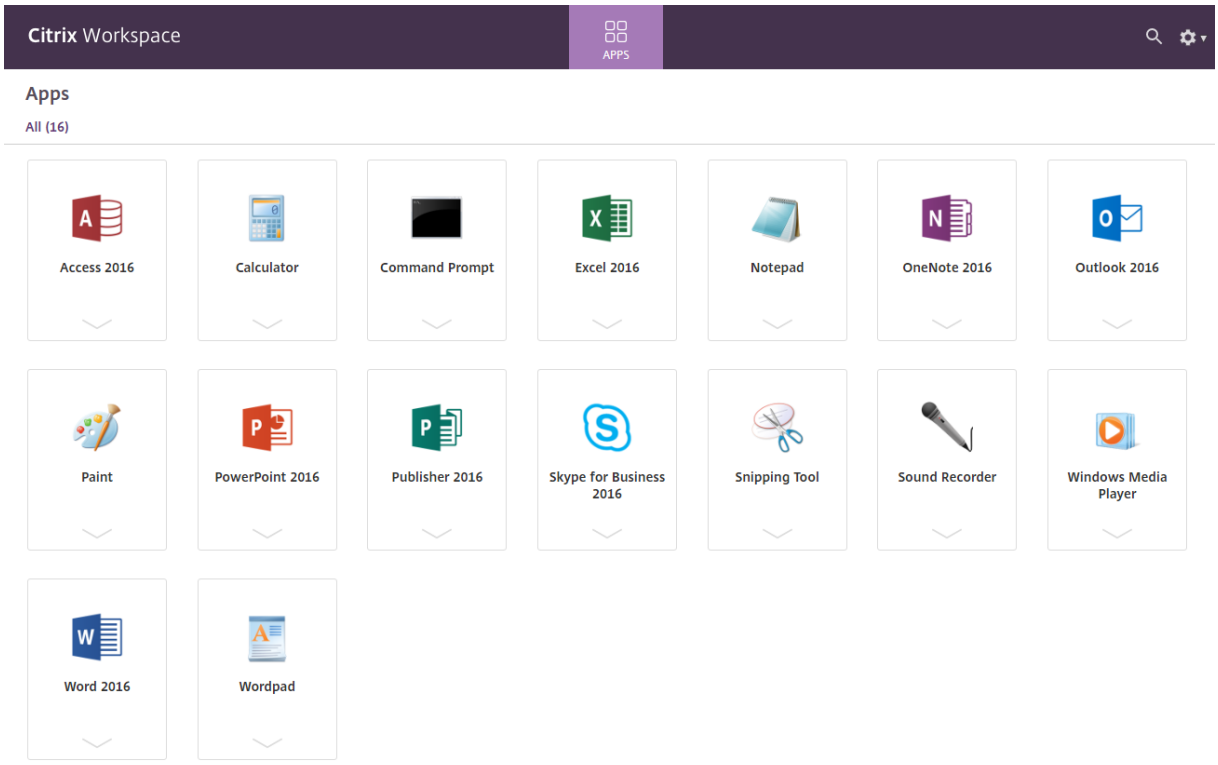
Citrix Workspace app for Windows supports configuring Workspace for subscribers, who might be using one or more services available from Citrix Cloud.

Citrix Workspace app intelligently displays only the specific workspace resources to which users are entitled. All your digital workspace resources available in Citrix Workspace app are powered by the Citrix Cloud Workspace experience service.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

A workspace is part of a digital workspace solution that enables IT to securely deliver access to apps from any device.

This screenshot is an example of what the workspace experience looks like to your subscribers. This interface is evolving and might look different to what your subscribers are working with today. For example, it might say "StoreFront"at the top of the page instead of "Workspace".



SaaS apps

Secure access to SaaS applications provides a unified user experience that delivers published SaaS applications to the users. SaaS apps are available with single sign-on. Administrators can now protect the organization's network and end-user devices from malware and data leaks. Administrators can achieve this by filtering access to specific websites and website categories.

Citrix Workspace app for Windows support the use of SaaS apps using the Citrix Secure Private Access. The service enables administrators to provide a cohesive experience, integrating single sign-on, and content inspection.

Delivering SaaS apps from the cloud has the following benefits:

- Simple configuration –Easy to operate, update, and consume.
- Single sign-on –Hassle-free log on with single sign-on.
- Standard template for different apps –Template-based configuration of popular apps.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Citrix Workspace app launches the SaaS apps on Citrix Enterprise Browser (formerly Citrix Workspace Browser). For information, see Citrix Enterprise Browser documentation.

Limitations:

1. When you launch a published app with the print option enabled and download disabled, and give a print command on a launched app, you can still save the PDF. As a workaround, to strictly disable the download functionality, disable the print option.
2. Videos embedded in an app might not work.

For more information about StoreFront Cloud, see StoreFront Cloud in Citrix Cloud.

PDF printing

Citrix Workspace app for Windows supports PDF printing in a session. The Citrix PDF Universal Printer driver allows you to print documents that are launched using hosted applications and desktops running on Citrix Virtual Apps and Desktops and Citrix DaaS.

When you select the **Citrix PDF Printer** option from the **Print** dialog, the printer driver converts the file to a PDF and transfers the PDF to the local device. The PDF is then launched using the default PDF viewer for viewing and prints from a locally attached printer.

Citrix recommends the Google Chrome browser or Adobe Acrobat Reader for PDF viewing.

You can enable Citrix PDF printing using Citrix Studio on the Delivery Controller.

Prerequisites:

- Citrix Workspace app Version 1808 or later.
- Citrix Virtual Apps and Desktops Version 7 1808 or later.
- At least one PDF viewer must be installed on your computer.

To enable PDF printing:

1. On the Delivery Controller, use the Citrix Studio, to select the **Policy** node in the left pane. You can either create a policy or edit an existing policy.
2. Set the **Auto-create PDF Universal Printer** policy to Enabled.

Restart the Citrix Workspace app session for the changes to take effect.

Limitation:

- PDF viewing and printing aren't supported on the Microsoft Edge browser.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Expanded tablet mode in Windows 10 using Windows Continuum

Windows Continuum is a Windows 10 feature that adapts to the way the client device is used. Citrix Workspace app for Windows Version 4.10 and later supports Windows Continuum, including dynamic change of modes.

For touch-enabled devices, the Windows 10 VDA starts in tablet mode when there's no keyboard or mouse attached. It starts in desktop mode when either a keyboard or a mouse or both are attached. Detaching or attaching the keyboard on any client device or the screen on a 2-in-1 device like a Surface Pro toggles between tablet and desktop modes. For more information, see Tablet mode for touch-screen devices in Citrix Virtual Apps and Desktops documentation.

On a touch-enabled client device, the Windows 10 VDA detects the presence of a keyboard or mouse when you connect or reconnect to a session. It also detects when you attach or detach a keyboard or mouse during the session. This feature is enabled by default on the VDA. To disable the feature, modify the **Tablet mode toggle** policy using Citrix Studio.

Tablet mode offers a user interface that is better suited to touchscreens:

- Slightly larger buttons.
- The **Start** screen and all the apps you start open in a full screen.
- The taskbar includes a Back button.
- Icons are removed from the taskbar.

Desktop mode offers the traditional user interface where you interact in the same manner as a PC with a keyboard and mouse.

> **Note:**
>
> Workspace for web doesn't support the Windows Continuum feature.

Citrix Analytics

Citrix Workspace app is instrumented to securely transmit logs to Citrix Analytics. The logs are analyzed and stored on Citrix Analytics servers when enabled. For more information about Citrix Analytics, see Citrix Analytics.

Relative mouse

The relative mouse feature determines how far the mouse has moved since the last frame within a window or screen.
The relative mouse uses the pixel delta between the mouse movements. When you change, for example, the direction of the camera using mouse controls, the feature is efficient. Apps also often hide

© 1997–2026 Citrix Systems, Inc. All rights reserved.

the mouse cursor because the position of the cursor relative to the screen coordinates isn't relevant, when manipulating a 3-D object or scene.

Relative mouse support provides an option to interpret the mouse position in a relative rather than an absolute manner. The interpretation is required for applications that demand relative mouse input rather than absolute.

You can configure the feature both on a per-user and a per-session basis, which gives more granular control on the feature availability.

> **Note**
>
> This feature can be applied in a published desktop session only.

Configuring the feature using the Registry Editor or the default.ica file allows the setting to be persistent even after the session is terminated.

Configuring relative mouse using the Registry editor

To configure the feature, set the following registry keys as applicable and then restart the session for the changes to take effect:

To make the feature available on a per-session basis:
`HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Citrix\ICA Client\Engine\Lockdown Profiles\All Regions\Lockdown\Virtual Channels\RelativeMouse`

To make the feature available on a per-user basis:
`HKEY_CURRENT_USER\Software\Policies\Citrix\ICA Client\Engine\Lockdown Profiles\All Regions\Lockdown\Virtual Channels\RelativeMouse`

- Name: Mouse
- Type: REG_SZ
- Value: True

> **Note:**
>
> - The values set in the Registry editor take precedence over the ICA file settings.
> - The values set in HKEY_LOCAL_MACHINE and HKEY_CURRENT_USER must be the same. Different values might cause conflicts.

Configuring the relative mouse using the default.ica file

1. Open the default.ica file typically at `C:\inetpub\wwwroot\Citrix\<site name>\conf\default.ica`, where sitename is the name specified for the site while creating. For

© 1997–2026 Citrix Systems, Inc. All rights reserved.

StoreFront customers, the default.ica file is typically at `C:\inetpub\wwwroot\Citrix\<Storename>\App_Data\default.ica`, where `storename` is the name set for the store when created.

2. Add a key by name RelativeMouse in the WFClient section. Set its value to the same configuration as the JSON object.
3. Set the value as required:
    - true –To enable relative mouse
    - false –To disable relative mouse
4. Restart the session for the changes to take effect.

> **Note:**
>
> The values set in the Registry editor take precedence over the ICA file settings.

Enabling relative mouse from the Desktop Viewer

1. Log on to Citrix Workspace app.
2. Launch a published desktop session.
3. From the Desktop Viewer toolbar, select **Preferences**.

   The Citrix Workspace - Preferences window appears.
4. Select **Connections**.
5. Under **Relative Mouse** settings, enable **Use relative mouse**.
6. Click **Apply** and **OK.**

> **Note:**
>
> Configuring the relative mouse from the Desktop Viewer applies the feature to per-session only.

Hardware decoding

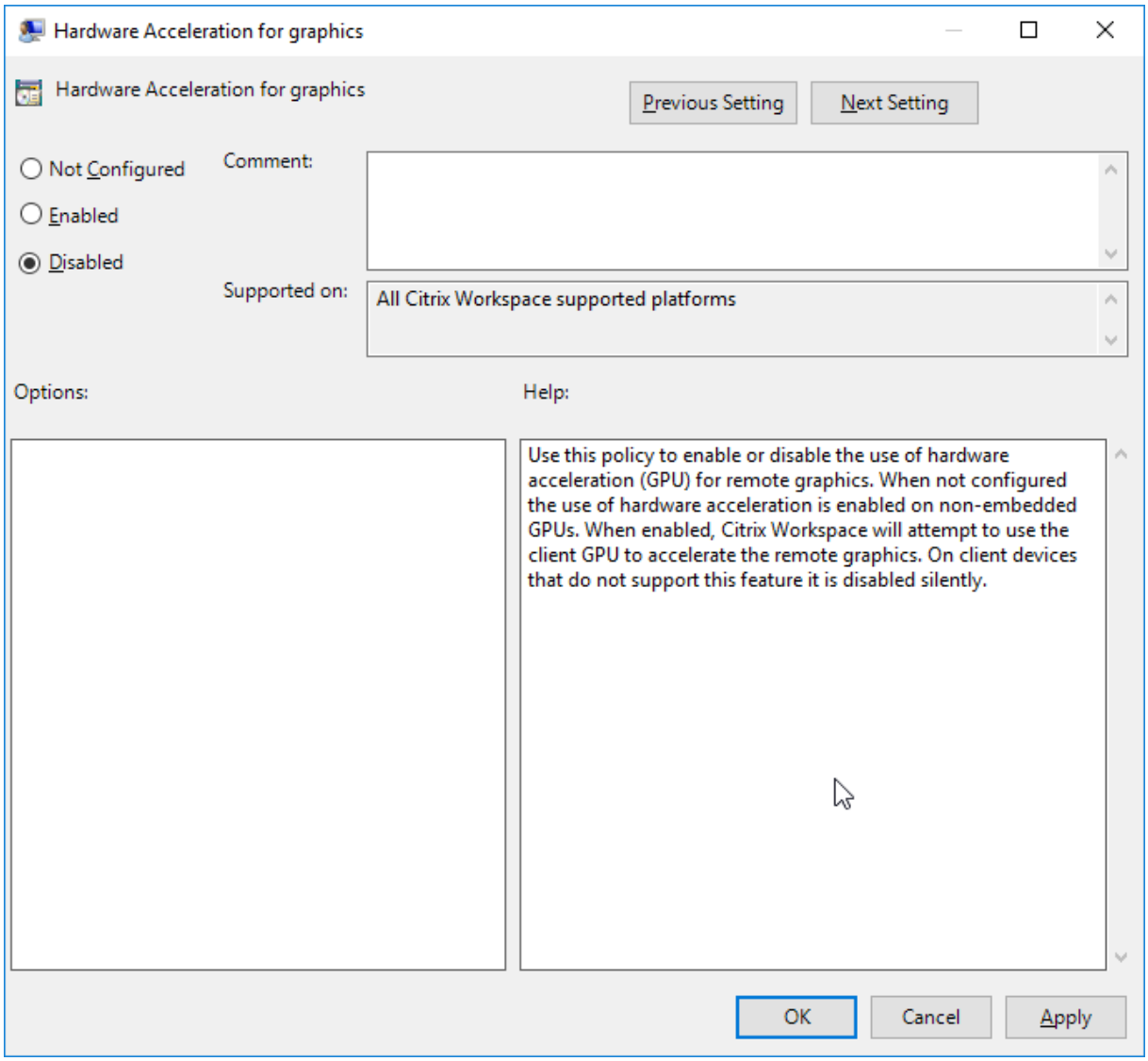
When using Citrix Workspace app (with HDX engine 14.4), the GPU can be used for H.264 decoding wherever it's available at the client. The API layer used for GPU decoding is DirectX Video Acceleration.

To enable hardware decoding using Citrix Workspace app Group Policy Object administrative template:

1. Open the Citrix Workspace app Group Policy Object administrative template by running gpedit.msc.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

2. Under the **Computer Configuration** node, go to **Administrative Templates** > **Citrix Workspace** >**User Experience.**
3. Select **Hardware Acceleration for graphics**.
4. Select **Enabled** and click **Apply** and **OK**.



To validate if the policy is set and hardware acceleration is used for an active ICA session, check the following registry entries:

Registry Path: `HKEY_CURRENT_USER\SOFTWARE\Citrix\ICA Client\CEIP\Data\GfxRender`.

> **Tip**
>
> The value for **Graphics_GfxRender_Decoder** and **Graphics_GfxRender_Renderer** must be 2. If the value is 1, that means CPU-based decoding is being used.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

When using the hardware decoding feature, consider the following limitations:

- If the client has two GPUs and if one of the monitors is active on the second GPU, CPU decoding is used.
- When connecting to a Citrix Virtual Apps server running on Windows Server 2008 R2, don't use hardware decoding on the user's Windows device. If enabled, issues like slow performance while highlighting text and flickering issues are seen.

Microphone input

Citrix Workspace app supports multiple client-side microphone inputs. You can use locally installed microphones for:

- Real-time activities, such as softphone calls and Web conferences.
- Hosted recording applications, such as dictation programs.
- Video and audio recordings.

Citrix Workspace app users can select whether to use microphones attached to their device using Connection Center. Citrix Virtual Apps and Desktops and Citrix DaaS users can also use the Citrix Virtual Apps and Desktops viewer Preferences to disable their microphones and webcams.

Client drive-mapping

Client drive mapping supports the transfer of data between the host and the client as a stream. The file transfer adapts to the changing network throughput conditions. It also uses any available extra bandwidth to scale up the data transfer rate.

By default, this feature is enabled.

To disable this feature, set the following registry key and then restart the server:

Path: `HKEY_LOCAL_MACHINE\System\Currentcontrolset\services\picadm\Parameters`
Name: `DisableFullStreamWrite`
Type: REG_DWORD
Value:
`0x01` - disables
`0` or delete - enables

Multi-monitor support

You can use up to eight monitors with Citrix Workspace app for Windows.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Each monitor in a multiple monitor configuration has its own resolution designed by its manufacturer. Monitors can have different resolutions and orientations during sessions.

Sessions can span multiple monitors in two ways:

- Full screen mode, with multiple monitors shown inside the session; applications snap to monitors as they would locally.

  Citrix Virtual Apps and Desktops and Citrix DaaS: To display the Desktop Viewer window across any rectangular subset of monitors, resize the window across any part of those monitors and click **Maximize**.

- Windowed mode, with one single monitor image for the session, applications do not snap to individual monitors.

Citrix Virtual Apps and Desktops and Citrix DaaS: When any desktop in the same assignment (formerly "desktop group") is launched then, the window setting is preserved and the desktop is displayed across the same monitors. Multiple virtual desktops can be displayed on one device provided the monitor arrangement is rectangular. If the primary monitor on the device is used by the virtual apps and desktops session, it becomes the primary monitor in the session. Otherwise, the numerically lowest monitor in the session becomes the primary monitor.

To enable multi-monitor support, check the following:

- The user device is configured to support multiple monitors.
- The operating system can detect each of the monitors. On Windows platforms, to verify that this detection occurs, go to **Settings** > **System** and click **Display** and confirm that each monitor appears separately.
- After your monitors are detected:
  - **Citrix Virtual Desktops™:** Configure the graphics memory limit using the **Citrix Machine Policy** setting Display memory limit.
  - **Citrix Virtual Apps:** Depending on the version of the Citrix Virtual Apps server, you've installed:
    - Configure the graphics memory limit using the **Citrix Computer Policy** setting Display memory limit.
    - From the Citrix management console for the Citrix Virtual Apps server, select the farm and in the task pane, select:
      - **Modify Server Properties** > **Modify all properties** > **Server Default** > **HDX Broadcast** > **Display** or
      - **Modify Server Properties** > **Modify all properties** > **Server Default** > **ICA** > **Display**) and
    - Set the Maximum memory to use for each session's graphics.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Check if the setting is large enough (in kilobytes) to provide sufficient graphic memory. If this setting isn't high enough, the published resource is restricted to the subset of the monitors that fits within the size specified.

Using Citrix Virtual desktops on dual monitor:

1. Select the Desktop Viewer and click the down arrow.
2. Select **Window**.
3. Drag the Citrix Virtual Desktops screen between the two monitors. Ensure that about half the screen is present in each monitor.
4. From the Citrix Virtual Desktop toolbar, select **Full-screen**.

   The screen is now extended to both the monitors.

For calculating the session's graphic memory requirements for Citrix Virtual Apps and Desktops and Citrix DaaS, see Knowledge Center article CTX115637.

Printer

To override the printer settings on the user device

1. From the **Print** menu available from an application on the user device, choose **Properties**.
2. On the **Client Settings** tab, click Advanced Optimizations and modify the Image Compression and Image and Font Caching options.

On-screen keyboard control

To enable touch-enabled access to virtual applications and desktops from Windows tablets, Citrix Workspace app automatically displays the on-screen keyboard when:

- you activate a text entry field and
- when the device is in tent or tablet mode.

On some devices and in some circumstances, Citrix Workspace app can't accurately detect the mode of the device. The on-screen keyboard might also appear when you don't want it to.

To suppress the on-screen keyboard from appearing when using a convertible device:

- create a REG_DWORD value DisableKeyboardPopup in `HKEY\\_CURRENT\\_USER\\SOFTWARE\\Citrix\\ICA Client\\Engine\\Configuration\\Advanced\\Modules\\MobileReceiver` and
- set the value to 1.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

> **Note:**
>
> On a x64 machine, create the value in HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Citrix\ICA Client\Engine\Configuration\Advanced\Modules\MobileReceiver.

The keys can be set to the following 3 different modes:

- **Automatic**: AlwaysKeyboardPopup = 0; DisableKeyboardPopup = 0
- **Always popup** (on-screen keyboard): AlwaysKeyboardPopup = 1; DisableKeyboardPopup = 0
- **Never popup** (on-screen keyboard): AlwaysKeyboardPopup = 0; DisableKeyboardPopup = 1

Keyboard shortcuts

You can configure combinations of keys that Citrix Workspace app interprets as having special functionality. When the keyboard shortcuts policy is enabled, you can specify Citrix Hotkey mappings, behavior of Windows hotkeys, and keyboard layout for sessions.

1. Open the Citrix Workspace app Group Policy Object administrative template by running gpedit.msc.
2. Under the **Computer Configuration node**, go to **Administrative Templates**> **Citrix Components** > **Citrix Workspace** > **User Experience**.
3. Select the Keyboard shortcuts policy.
4. Select **Enabled**, and the required options.
5. Restart the Citrix Workspace app session for the changes to take effect.

Citrix Workspace app support for 32-bit color icons:

Citrix Workspace app supports 32-bit high color icons. To provide for seamless applications, it automatically selects the color depth for:

- applications visible in the **Connection Center** dialog,
- the Start menu, and
- task bar

> **Caution**
>
> Editing the registry incorrectly can cause serious problems that might require you to reinstall your operating system. Citrix can't guarantee that problems resulting from the incorrect use of the Registry Editor can be solved. Use the Registry Editor at your own risk. Be sure to back up the registry before you edit it.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

To set a preferred depth, you can add a string registry key named `TWIDesiredIconColor` to `HKEY\\_LOCAL\\_MACHINE\SOFTWARE\Wow6432Node\Citrix\ICA Client\Engine\Lockdown Profiles\All Regions\Preferences` and set it to the required value. The possible color depths for icons are 4, 8, 16, 24, and 32 bits-per-pixel. The user can select a lower color depth for icons if the network connection is slow.

Desktop Viewer

Different enterprises might have different corporate needs. Your requirements for the way users access virtual desktops might vary from user to user and as your corporate needs evolve. The user experience of connecting to virtual desktops and the extent at which the user can configure the connections depend Citrix Workspace app for Windows setup.

Use the **desktop viewer** when users need to interact with their virtual desktop. The user's virtual desktop can be a published virtual desktop, or a shared or dedicated desktop. In this access scenario, the **Desktop Viewer** toolbar functionality allows the user to open a virtual desktop in a window and pan and scale that desktop inside their local desktop. Users can set preferences and work on more than one desktop using multiple Citrix Virtual Apps and Desktops and Citrix DaaS connections on the same user device.

> **Note:**
>
> Use Citrix Workspace app to change the screen resolution on their virtual desktops. You can't change Screen Resolution using the Windows Control Panel.

Keyboard input in Desktop Viewer

In Desktop Viewer sessions, the **Windows logo** key+L is directed to the local computer.

Ctrl+Alt+Delete is directed to the local computer.

Key presses that activate certain Microsoft accessibility features, for example, Sticky Keys, Filter Keys, and Toggle Keys are normally directed to the local computer.

As an accessibility feature of the Desktop Viewer, pressing Ctrl+Alt+Break displays the **Desktop Viewer** toolbar buttons in a pop-up window.

Ctrl+Esc is sent to the remote, virtual desktop.

> **Note:**
>
> By default, if the Desktop Viewer is maximized, Alt+Tab switches focus between windows inside the session. If the Desktop Viewer is displayed in a window, Alt+Tab switches focus between windows outside the session.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Hotkey sequences are key combinations designed by Citrix. Hotkey sequences are, for example, the Ctrl+F1 sequence reproduces Ctrl+Alt+Delete, and Shift+F2 switches applications between full-screen and windowed mode.

> **Note:**
>
> You can't use hotkey sequences with virtual desktops displayed in the Desktop Viewer, that is, with virtual apps and desktops sessions. However, you can use them with published applications, that is, with virtual apps sessions.

Virtual desktops

From within a desktop session, users can't connect to the same virtual desktop. If the user tries do so, disconnects the existing desktop session. So, Citrix recommends:

- Administrators must not configure the clients on a desktop to point to a site that publishes the same desktop
- Users must not browse site that hosts the same desktop if the site is configured to automatically reconnect users to existing sessions
- Users must not browse to a site that hosts the same desktop and try to launch it

A user who logs on locally to a computer that is acting as a virtual desktop, blocks connection to that desktop.

Citrix recommends working with them to define device mapping:

- if your users connect to virtual applications, published with Citrix Virtual Apps, from a virtual desktop and
- your organization has a separate Citrix Virtual Apps administrator.

Device mapping checks if the desktop devices are mapped consistently within desktop and application sessions. Because local drives are displayed as network drives in desktop sessions, the Citrix Virtual Apps administrator needs to change the drive-mapping policy to include network drives.

Status indicator time-out

You can change the amount of time the status indicator displays when a user is launching a session.

To alter the time-out period, do the following steps:

1. Launch the Registry Editor.
2. Navigate to the following path:
    - On a 64-bit: `HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Citrix\ICA CLIENT\Engine`

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- On a 32-bit: HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\ICA CLIENT\Engine\

3. Create a registry key as follows:

   - Type: REG_DWORD
   - Name: SI INACTIVE MS
   - Value: 4, if you want the status indicator to disappear sooner.

When you configure this key, the status indicator might appear and disappear frequently. This behavior is as designed. To suppress the status indicator, do the following:

1. Launch the Registry Editor.
2. Navigate to the following path:

   - On a 64-bit: HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Citrix\ICA CLIENT\
   - On a 32-bit: HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\ICA CLIENT\

3. Create a registry key as follows:

   - Type: REG_DWORD
   - Name: NotificationDelay
   - Value: Any value in millisecond (for example, 120000)

Inactivity Timeout for Workspace Sessions

Admins can configure the inactivity timeout value to specify the amount of idle time allowed before the users automatically sign out of the Citrix Workspace session. You're automatically signed out of Workspace if the mouse, keyboard, or touch is idle for the specified interval of time. The inactivity timeout doesn't affect the active virtual apps and desktops sessions or Citrix StoreFront stores.

The inactivity timeout value can be set starting from a 1 minute to 1,440 minutes. By default, the inactivity timeout isn't configured. Admins can configure the inactivityTimeoutInMinutes property by using a PowerShell module. Click here to download the PowerShell modules for Citrix Workspace Configuration.

The end-user experience is as follows:

- A notification appears in your session window three minutes before you're signed out, with an option to stay signed in, or sign out.
- The notification appears only if the configured inactivity timeout value is greater than or equal to five minutes.
- Users can click **Stay signed in** to dismiss the notification and continue using the app, in which case the inactivity timer is reset to its configured value. You can also click **Sign out** to end the session for the current store.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

> **Note:**
>
> Admins can configure the inactivity timeout only for Workspace (cloud) sessions.

Customer Experience Improvement Program (CEIP)

Data collected	Description	What we use it for
Configuration and usage data	The Citrix Customer Experience Improvement Program (CEIP) gathers configuration and usage data from Citrix Workspace app for Windows and automatically sends the data to Citrix and Google Analytics.	This data helps Citrix improve the quality, reliability, and performance of Citrix Workspace app.

> **Note:**
>
> Starting with version 2203.1 LTSR CU4, the Citrix Workspace app doesn't collect any CEIP data from users located in the European Union (EU), European Economic Area (EEA), Switzerland, and United Kingdom (UK). Update your Citrix Workspace app if you wish to take advantage of this functionality.

Additional information

Citrix handles your data according to the terms of your contract with Citrix, and protect it as specified in the Citrix Services Security Exhibit. Citrix Services Security Exhibit is available on the Citrix Trust Center.

Citrix also uses Google Analytics to collect certain data from Citrix Workspace app as part of CEIP. Review how Google handles data collected for Google Analytics.

You can stop sending CEIP data to Citrix and Google Analytics by:

1. Right-click the Citrix Workspace app icon from the notification area.
2. Select **Advanced Preferences**.
   The **Advanced Preferences** dialog appears.
3. Select **Data Collection**.
4. Select **No, Thanks** to disable CEIP or to forego participation.
5. Click **Save**.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

> **Note:**
>
> You can stop sending CEIP data except for the operating system and Citrix Workspace app versions collected for Google Analytics indicated by an * in the second table.

You can also navigate to the following registry entry and set the value as suggested:

Path: `HKEY_LOCAL_MACHINE\ SOFTWARE\Citrix\ICA Client\CEIP`

Key: `Enable_CEIP`

Value: `False`

> **Note:**
>
> Once you select **No Thanks** or set the `Enable_CEIP` key to `False`, to stop sending the final two CEIP data elements, that is, Operating System and Citrix Workspace app version, navigate to the following registry entry and set the value:

Path: `HKEY_LOCAL_MACHINE\ SOFTWARE\Citrix\ICA Client\CEIP`

Key: `DisableHeartbeat`

Value: `True`

The specific CEIP data elements collected by Citrix are:

Operating system version	Citrix Workspace app version	External devices connected	Screen resolution
Flash version	Desktop Lock configuration	Touch enabled	Authentication configuration
Session launch method	Graphics configuration	Desktop Viewer configuration	Printing
Connection error	Time to launch	Citrix Workspace app language	VDA information
SSON state	Installer state	Time to install	Connection protocol
Internet Explorer version			

The specific CEIP data elements collected by Google Analytics are:

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Operating system version*	Citrix Workspace app version*	Authentication configuration	Citrix Workspace app language
Session launch method	Connection error	Connection protocol	VDA information
Installer configuration	Installer state	Client keyboard layout	Store configuration
Auto-update preference	Connection Center usage	App Protection configuration	Reason for the offline banner

Regional settings

Citrix Workspace app displays the date, time, and number based on the locale of the browser or endpoint device.

Starting from Citrix Workspace app 2106, you can customize regional date, time, and number formats through Regional Settings. Changes made in these settings are saved for an individual user and applied across all devices.

> **Note:**
>
> This option is available only on Cloud deployments.

For more information, see Regional Settings.

Configuring single sign-on to Citrix Workspace app

July 17, 2026

Single sign-on using Azure Active Directory

This section explains how to implement single sign-on (SSO) using Azure Active Directory (AAD) as an identity provider with domain joined workloads in hybrid or AAD enrolled endpoints. With this configuration, you can authenticate to Workspace using Windows Hello or FIDO2 on endpoints that are enrolled to AAD.

> **Note:**
>
> If you use Windows Hello, as a standalone authentication, you can achieve single sign-on to Citrix

© 1997–2026 Citrix Systems, Inc. All rights reserved.

> Workspace app. However, you are prompted for your user name and password while accessing published virtual apps or desktops. As a workaround, consider implementing Federated Authentication Service (FAS).

Prerequisites

- An active Azure Active Directory connection to Citrix Cloud. For more information, see Connect Azure Active Directory to Citrix Cloud.
- An Azure Active Directory workspace authentication. For more information, see Enable Azure AD authentication for workspaces.
- Verify if you have configured Azure AD Connect. For more information, see Getting started with Azure AD Connect using express settings.
- Activate Pass-through authentication on Azure AD Connect. Also, verify if the single sign-on and the Pass-through options work on the Azure portal. For more information, see Azure Active Directory Pass-through Authentication: Quickstart.

Configuration

Do the following steps to configure SSO on your device:

1. Install the Citrix Workspace app using the Windows command line with the `includeSSON` option:

```
CitrixWorkspaceApp.exe /includeSSON
```

1. Reboot your device.
2. Open the Citrix Workspace app Group Policy Object administrative template by running `gpedit.msc`.
3. Go to **Administrative Templates** > **Citrix Components** > **Citrix Workspace** > **User Authentication** > **Local user name and password**.
4. Select **Enable pass-through authentication**. Depending on the configuration and security settings, select the **Allow pass-through authentication for all ICA®** option for pass-through authentication to work.
5. Modify the User Authentication settings in Internet Explorer. To modify the settings:
    - Open **Internet Properties** from the Control panel.
    - Navigate to **General Properties** > **Local Intranet** and click **Sites**.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- In the **Local Intanet** window, click **Advanced, add trusted sites**, add the following trusted sites, and click **Close**:
  - `https://aadg.windows.net.nsatc.net`
  - `https://autologon.microsoftazuread-sso.com`
  - `The name of your tenant, for example: https://xxxtenantxxx.cloud.com`

6. Disable extra authentication prompts by disabling the `prompt=login` attribute in your tenant. For more information, see User Prompted for Additional Credentials on cloud store URLs When Using Federated Authentication Providers. You can contact Citrix technical support to disable the `prompt=login` attribute in your tenant to successfully configure single sign-on.
7. Enable domain pass-through authentication on the Citrix Workspace app client. For more information, see Domain pass-through authentication.
8. Restart the Citrix Workspace app for the changes to take effect.

Single sign-on using Okta and Federated Authentication Service

This section explains how you can implement single sign-on (SSO) using Okta as an identity provider with domain joined device and Federated Authentication Service (FAS). With this configuration, you can authenticate to Workspace using Okta to enable single sign-on and prevent a second logon prompt. For this authentication mechanism to work, you need to use the Citrix Federated Authentication Service with Citrix Cloud. For more information, see Connect Citrix Federated Authentication Service to Citrix Cloud.

Prerequisites

- Cloud Connector. For more information about installing the Cloud Connector, see Cloud Connector Installation.
- An Okta agent. For more information about installing an Okta agent, see Install the Okta Active Directory agent. Also, you can cofigure the Okta IWA Web agent to login from a Windows Domain joined device. For more information, see Install and configure the Okta IWA Web agent for Desktop single sign-on
- An active Azure Active Directory connection to Citrix Cloud. For more information, see Connect Azure Active Directory to Citrix Cloud.
- Federated Authentication Service. For more information, see Install the Federated Authentication Service.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Configuration

Do the following steps to configure SSO on your device:

Connect Citrix Cloud™ to your Okta organization:

1. Download and install the Okta Active Directory agent. For more information, see Install the Okta Active Directory agent.
2. Sign in to Citrix Cloud at `https://citrix.cloud.com`.
3. From the Citrix Cloud menu, select **Identity and Access Management**.
4. Locate Okta and select **Connect** from the ellipsis menu.
5. In **Okta URL**, enter your Okta domain.
6. In **Okta API Token**, enter the API token for your Okta organization.
7. In **Client ID** and **Client Secret**, enter the client ID and secret from the OIDC web app integration you created earlier. To copy these values from the Okta console, select **Applications** and locate your Okta application. Under **Client Credentials**, use the **Copy to Clipboard** button for each value.
8. Click **Test and Finish**. Citrix Cloud verifies your Okta details and tests the connection.

Enable Okta authentication for workspaces:

1. From the Citrix Cloud menu, select **StoreFront Cloud** > **Authentication**.
2. Select **Okta**. When prompted, select **I understand the impact on the subscriber experience**.
3. Click **Accept** to accept the permissions request.

Enable Federated Authentication Service:

1. From the Citrix Cloud menu, select **StoreFront Cloud** and then select **Authentication**.
2. Click **Enable FAS**. This change might take up to five minutes to be applied to subscriber sessions.

Afterward, the Federated Authentication Service is active for all virtual app and desktop launches from Citrix Workspace.

When subscribers sign in to their workspace and launch a virtual app or desktop in the same resource location as the FAS server, the app or desktop starts without prompting for credentials.

> **Note:**
>
> If all FAS servers in a resource location are down or in maintenance mode, application launches

© 1997–2026 Citrix Systems, Inc. All rights reserved.

> succeed, but single sign-on isn't active. Subscribers are prompted for their AD credentials to access each application or desktop.

Authenticate

December 5, 2025

To maximize the security of your environment, you must secure the connections between Citrix Workspace app and the resources you publish. You can configure various types of authentication for your Citrix Workspace app, including domain pass-through, smart card, and Kerberos pass-through.

Domain pass-through authentication

Single sign-on lets you authenticate to a domain and use Citrix Virtual Apps and Desktops™ and Citrix DaaS (formerly Citrix Virtual Apps and Desktops service) without having to reauthenticate again.

When you log on to Citrix Workspace app, your credentials are passed through to StoreFront, along with the apps and desktops and Start menu settings. After configuring single sign-on, you can log on to Citrix Workspace app and launch virtual apps and desktops sessions without having to retype your credentials.

All web browsers require you to configure single sign-on using the Group Policy Object(GPO) administrative template. For more information about configuring single sign-on using the Group Policy Object (GPO) administrative template, see Configure single sign-on with Citrix Gateway.

You can configure single sign-on on both fresh installation or upgrade setup, using any of the following options:

- Command-line interface
- GUI

Configure single sign-on during fresh installation

To configure single sign-on during fresh installation, do the following steps:

1. Configuration on StoreFront.
2. Configure XML trust services on the Delivery Controller.
3. Modify Internet Explorer settings.
4. Install Citrix Workspace app with single sign-on.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Configure single sign-on on StoreFront

Single sign-on lets you authenticate to a domain and use Citrix Virtual Apps and Desktops and Citrix DaaS from the same domain without having to reauthenticate to each app or desktop.

When you add a store using the **Storebrowse** utility, your credentials pass through the Citrix Gateway server, along with the apps and desktops enumerated for you, including your Start menu settings. After configuring single sign-on, you can add the store, enumerate your apps and desktops, and launch the required resources without having to type your credentials multiple times.

Depending on the Citrix Virtual Apps and Desktops deployment, single sign-on authentication can be configured on StoreFront using the Management Console.

Use the following table for different use cases and its respective configuration:

Use case	Configuration details	Additional information
Configured SSON on StoreFront	Launch Citrix Studio, go to **Stores** > **Manage Authentication Methods - Store** > enable **Domain pass-through**.	When Citrix Workspace app isn't configured with single sign-on, it automatically switches the authentication method from **Domain pass-through** to **User name and password**, if available.
When workspace for web is required	Launch **Stores** > **Workspace for Web Sites** > **Manage Authentication Methods - Store** > enable **Domain pass-through**.	When Citrix Workspace app isn't configured with single sign-on, it automatically switches the authentication method from **Domain pass-through** to **User name and password**, if available.

Configure single sign-on with Citrix Gateway

You enable single sign-on with Citrix Gateway using the Group Policy Object administrative template.

1. Open the Citrix Workspace app GPO administrative template by running `gpedit.msc`.
2. Under the **Computer Configuration node**, go to **Administrative Template** > **Citrix Components** > **Citrix Workspace** > **User Authentication**, and select **Single Sign-on for Citrix Gateway** policy.
3. Select **Enabled**.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

4. Click **Apply** and **OK**.
5. Restart Citrix Workspace app for the changes to take effect.

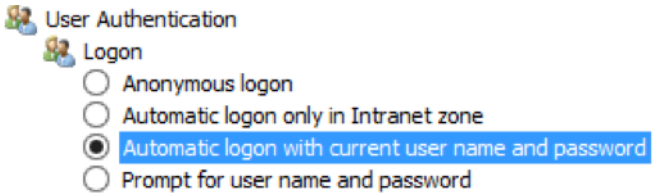
Configure XML trust services on the Delivery Controller

On Citrix Virtual Apps and Desktops and Citrix DaaS™, run the following PowerShell command as an administrator on the Delivery Controller:

```
asnp Citrix* ; Set-BrokerSite -TrustRequestsSentToTheXmlServicePort
$True
```

Modify the Internet Explorer settings

1. Add the StoreFront server to the list of trusted sites using Internet Explorer. To add:
   a) Launch **Internet Options** from the Control panel.
   b) Click **Security** > **Local Internet** and click **Sites**.
      The **Local intranet** window appears.
   c) Select **Advanced**.
   d) Add the URL of the StoreFront FQDN with the appropriate HTTP or HTTPS protocols.
   e) Click **Apply** and **OK**.
2. Modify the **User Authentication** settings in **Internet Explorer**. To modify:
   a) Launch **Internet Options** from the Control panel.
   b) Click **Security** tab > **Trusted Sites**.
   c) Click **Custom level**. The **Security Settings** –**Trusted Sites Zone** window appears.
   d) In the **User Authentication** pane, select **Automatic logon with current user name and password**.



   e) Click **Apply** and **OK**.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Configure single sign-on using the command-line interface

Install Citrix Workspace app with the /`includeSSON` switch and restart Citrix Workspace app for the changes to take effect.

> **Note:**
>
> When you install Citrix Workspace app for Windows without the single sign-on component, upgrade to the Citrix Workspace app latest version with the /`includeSSON` switch isn't supported.

Configure single sign-on using the GUI

1. Locate the Citrix Workspace app installation file (`CitrixWorkspaceApp.exe`).
2. Double-click `CitrixWorkspaceApp.exe` to launch the installer.
3. In the **Enable Single Sign-on installation** wizard, select the **Enable Single Sign-on** option.
4. Click **Next** and follow the prompts to complete the installation.

You can now log on to an existing store (or configure a new store) using Citrix Workspace app without entering user credentials.

Configure single sign-on on workspace for web

You can configure single sign-on on workspace for web using the Group Policy Object administrative template.

1. Open the workspace for web GPO administrative template by running gpedit.msc.
2. Under the **Computer Configuration** node, go to **Administrative Template** > **Citrix Component** > **Citrix Workspace** > **User Authentication**.
3. Select the **Local user name and password** policy and set it to **Enabled**.
4. Click **Enable pass-through authentication**. This option allows the workspace for web to use your login credentials for authentication on the remote server.
5. Click **Allow pass-through authentication for all ICA® connections**. This option bypasses any authentication restriction and allows credentials to pass-through on all the connections.
6. Click **Apply** and **OK**.
7. Restart the workspace for web for the changes to take effect.

Verify that the single sign-on is enabled by launching the **Task Manager** and check if the `ssonsvr.exe` process is running.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Configure single sign-on using Active Directory

Complete the following steps to configure Citrix Workspace app for pass-through authentication using Active Directory group policy. In this scenario, you can achieve the single sign-on authentication without using the enterprise software deployment tools, such as the Microsoft System Center Configuration Manager.

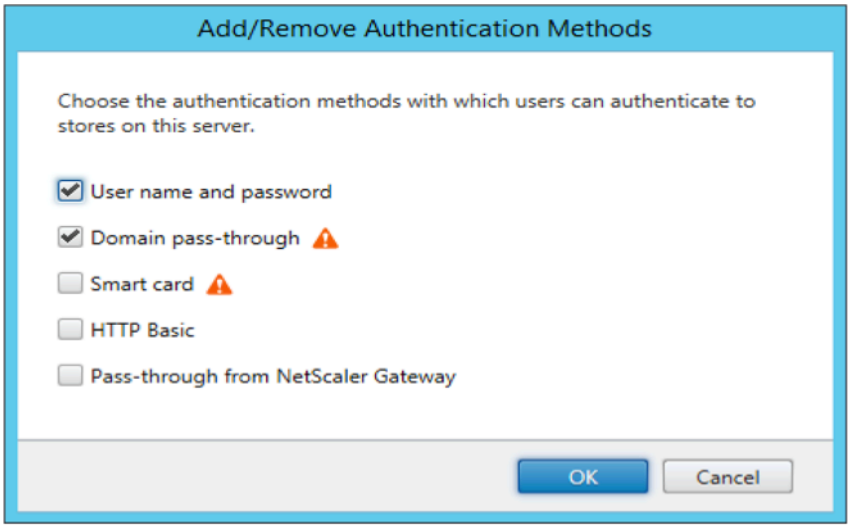
1. Download and place the Citrix Workspace app installation file (CitrixWorkspaceApp.exe) on a suitable network share. It must be accessible by the target machines you install Citrix Workspace app on.
2. Get the `CheckAndDeployWorkspacePerMachineStartupScript.bat` template from the Citrix Workspace app for Windows Download page.
3. Edit the content to reflect the location and the version of `CitrixWorkspaceApp.exe`.
4. In the **Active Directory Group Policy Management** console, type `CheckAndDeployWorkspacePerMac.bat` as a startup script. For more information on deploying the startup scripts, see the Active Directory section.
5. In the **Computer Configuration** node, go to **Administrative Templates > Add/Remove Templates** to add the `receiver.adml` file.
6. After adding the `receiver.adml` template, go to **Computer Configuration** > **Administrative Templates** > **Citrix Components** > **Citrix Workspace** > **User authentication**. For more information about adding the template files, see Group Policy Object administrative template.
7. Select the **Local user name and password** policy and set it to **Enabled**.
8. Select **Enable pass-through authentication** and click **Apply**.
9. Restart the machine for the changes to take effect.

Configure single sign-on on StoreFront

StoreFront configuration

1. Launch **Citrix Studio** on the StoreFront server and select **Stores** > **Manage Authentication Methods - Store**.
2. Select **Domain pass-through**.

© 1997–2026 Citrix Systems, Inc. All rights reserved.



Authentication tokens

Authentication tokens are encrypted and stored on the local disk so that you don't need to reenter your credentials when your system or session restarts. Citrix Workspace app provides an option to disable the storing of authentication tokens on the local disk.

For enhanced security, we now provide a Group Policy Object (GPO) policy to configure the authentication token storage.

> **Note:**
>
> This configuration is applicable only in cloud deployments.

To disable storing of authentication tokens using the Group Policy Object (GPO) policy:

1. Open the Citrix Workspace app Group Policy Object administrative template by running `gpedit.msc`.
2. Under the **Computer Configuration** node, go to **Administrative Templates** > **Citrix Components** > **SelfService**.
3. In the **Store authentication tokens** policy, select one of the following:
   - Enabled: Indicates that the authentication tokens are stored on the disk. By default, set to Enabled.
   - Disabled: Indicates that the authentication tokens aren't stored on the disk. Reenter your credentials when your system or session restarts.
4. Click **Apply** and **OK**.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Starting with Version 2106, Citrix Workspace app provides another option to disable the storing of authentication tokens on the local disk. Along with the existing GPO configuration, you can also disable the storing of authentication tokens on the local disk using the Global App Configuration Service.

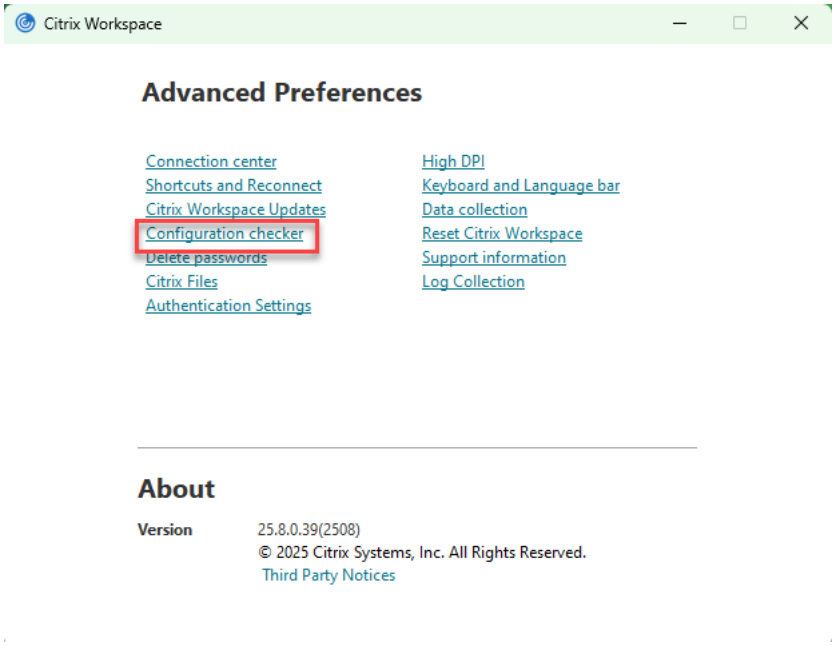
In the Global App Configuration Service, set the `Store Authentication Tokens` attribute to `False`.

For more information, see the Global App Configuration Service documentation.

Configuration Checker

Configuration Checker lets you run a test to check if the single sign-on is configured properly. The test runs on different checkpoints of the single sign-on configuration and displays the configuration results.

1. Right-click Citrix Workspace app icon in the notification area and click **Advanced Preferences**. The **Advanced Preferences** dialog appears.
2. Click **Configuration Checker**.
   The **Citrix Configuration Checker** window appears.



3. Select **SSONChecker** from the **Select** pane.
4. Click **Run**. A progress bar appears, displaying the status of the test.

The **Configuration Checker** window has the following columns:

1. **Status:** Displays the result of a test on a specific check point.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- A green check mark indicates that the specific checkpoint is configured properly.
- A blue I indicates information about the checkpoint.
- A Red X indicates that the specific checkpoint isn't configured properly.

2. **Provider:** Displays the name of the module on which the test is run. In this case, single sign-on.
3. **Suite:** Indicates the category of the test. For example, Installation.
4. **Test:** Indicates the name of the specific test that is run.
5. **Details:** Provides additional information about the test, for both pass and fail.

The user gets more information about each checkpoint and the corresponding results.

The following tests are done:

1. Installed with single sign-on.
2. Logon credential capture.
3. Network Provider registration: The test result against Network Provider registration displays a green check mark only when "Citrix Single Sign-on"is set to be first in the list of Network Providers. If Citrix Single Sign-on appears anywhere else in the list, the test result against Network Provider registration appears with a blue I and additional information.
4. Single sign-on process is running.
5. Group Policy: By default, this policy is configured on the client.
6. Internet Settings for Security Zones: Make sure that you add the Store/XenApp Service URL to the list of Security Zones in the Internet Options.
   If the Security Zones are configured via Group policy, any change in the policy requires the **Advanced Preferences** window to be reopened for the changes to take effect and to display the correct status of the test.
7. Authentication method for StoreFront.

> **Note:**
>
> - If you're accessing workspace for web, the test results aren't applicable.
> - If Citrix Workspace app is configured with multiple stores, the authentication method test runs on all the configured stores.
> - You can save the test results as reports. The default report format is .txt.

Hide the Configuration Checker option from the Advanced Preferences window

1. Open the Citrix Workspace app GPO administrative template by running `gpedit.msc`.
2. Go to **Citrix Components** > **Citrix Workspace** > **Self Service** > **DisableConfigChecker**.
3. Click **Enabled** to hide the **Configuration Checker** option from the **Advanced Preferences** window.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

4. Click **Apply** and **OK**.
5. Run the `gpupdate /force` command.

Limitation:

Configuration Checker does not include the checkpoint for the configuration of trust requests sent to the XML service on Citrix Virtual Apps and Desktops servers.

Beacon test Citrix Workspace app allows you to do a beacon test using the Beacon checker that is available as part of the **Configuration Checker** utility. The Beacon test helps to confirm if the beacon (ping.citrix.com) is reachable. This diagnostic test helps to eliminate one of the many possible causes for slow resource enumeration, that is the beacon not being available. To run the test, right-click the Citrix Workspace app in the notification area and select **Advanced Preferences** > **Configuration Checker**. Select the **Beacon checker** option from the list of Tests and click **Run**.

The test results can be any of the following:

- Reachable –Citrix Workspace app is successfully able to contact the beacon.
- Not reachable - Citrix Workspace app is unable to contact the beacon.
- Partially reachable - Citrix Workspace app can contact the beacon intermittently.

> **Note:**
>
> - The test results aren't applicable on workspace for web.
> - The test results can be saved as reports. The default format for the report is .txt.

Domain pass-through authentication with Kerberos

This topic applies only to connections between Citrix Workspace app for Windows and StoreFront, Citrix Virtual Apps and Desktops, and Citrix DaaS.

Citrix Workspace app supports Kerberos for domain pass-through authentication for deployments that use smart cards. Kerberos is one of the authentication methods included in **Integrated Windows Authentication (IWA)**.

When enabled, Kerberos authenticates without passwords for Citrix Workspace app. As a result, prevents Trojan horse-style attacks on the user device that try to gain access to passwords. Users can log on using any authentication method and access published resources, for example, a biometric authenticator such as a fingerprint reader.

When you log on using a smart card to Citrix Workspace app, StoreFront, Citrix Virtual Apps and Desktops and Citrix DaaS configured for smart card authentication- the Citrix Workspace app:

1. Captures the smart card PIN during single sign-on.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

2. Uses IWA (Kerberos) to authenticate the user to StoreFront. StoreFront then provides your Citrix Workspace app with information about available the Citrix Virtual Apps and Desktops and Citrix DaaS.

   > **Note**
   >
   > Enable Kerberos to avoid an extran PIN prompt. If Kerberos authentication isn't used, Citrix Workspace app authenticates to StoreFront using the smart card credentials.

3. The HDX engine (previously referred to as the ICA client) passes the smart card PIN to the VDA to log the user on to Citrix Workspace app session. Citrix Virtual Apps and Desktops and Citrix DaaS then delivers the requested resources.

To use Kerberos authentication with Citrix Workspace app, check if the Kerberos configuration conforms to the following.

- Kerberos works only between Citrix Workspace app and servers that belong to the same or to trusted Windows Server domains. Servers are trusted for delegation, an option you configure through the Active Directory Users and Computers management tool.
- Kerberos must be enabled both on the domain and Citrix Virtual Apps and Desktops and Citrix DaaS. For enhanced security and to make sure that Kerberos is used, disable any non-Kerberos IWA options on the domain.
- Kerberos logon isn't available for Remote Desktop Services connections that're configured to use either Basic authentication, always use specified logon information, or always prompt for a password.

> **Warning**
>
> Using the Registry editor incorrectly might cause serious problems that can require you to reinstall the operating system. Citrix can't guarantee that problems resulting from incorrect use of the Registry editor can be solved. Use the Registry Editor at your own risk. Make sure you back up the registry before you edit it.

Domain pass-through authentication with Kerberos for use with smart cards

Before continuing, see Secure your deployment section in the Citrix Virtual Apps and Desktops document.

When you install Citrix Workspace app for Windows, include the following command-line option:

- `/includeSSON`

  This option installs the single sign-on component on the domain-joined computer, enabling your workspace to authenticate to StoreFront using IWA (Kerberos). The single sign-on compo-

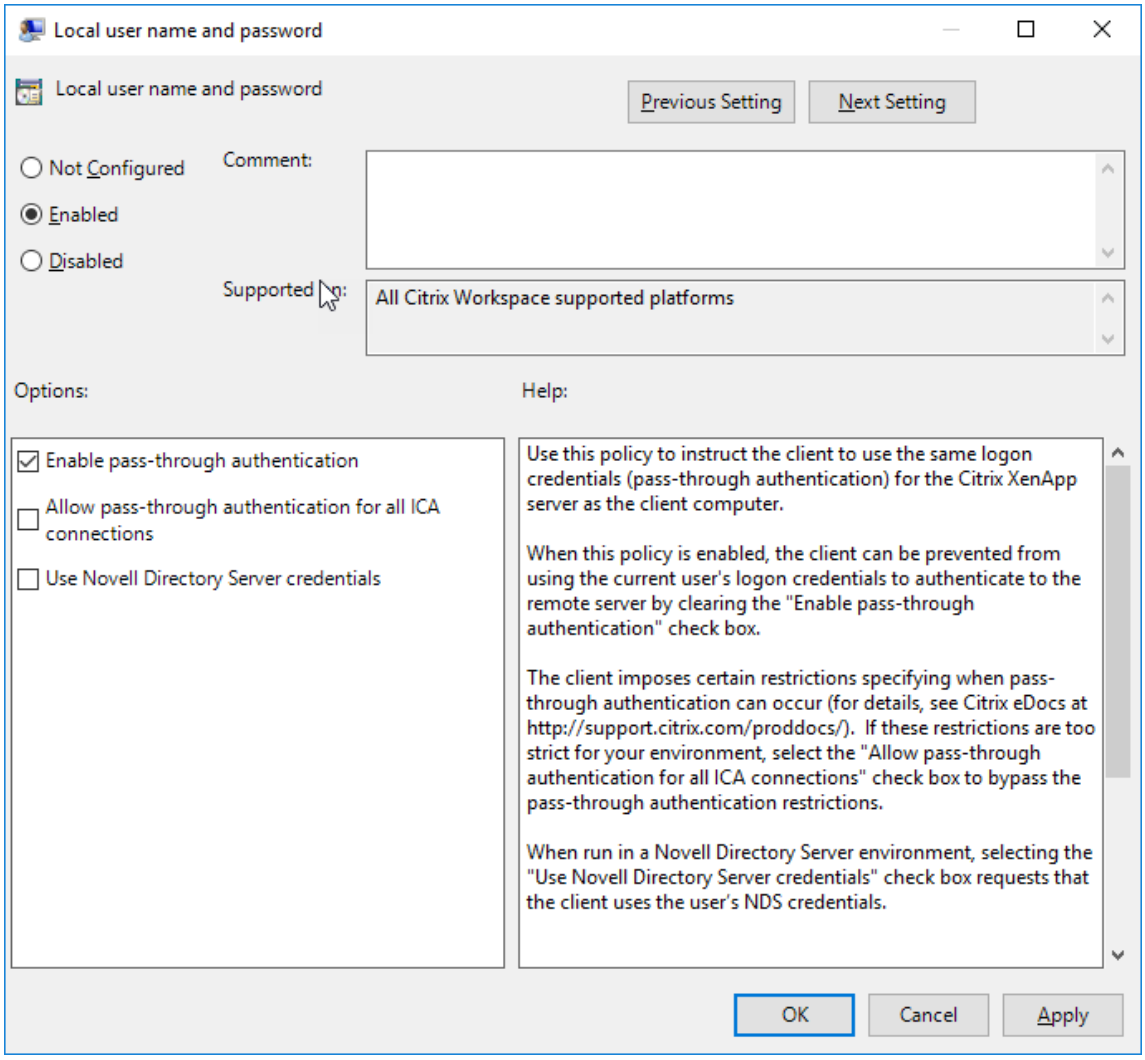
© 1997–2026 Citrix Systems, Inc. All rights reserved.

nent stores the smart card PIN, used by the HDX engine when it remotes the smart card hardware and credentials to Citrix Virtual Apps and Desktops and Citrix DaaS. Citrix Virtual Apps and Desktops and Citrix DaaS automatically selects a certificate from the smart card and gets the PIN from the HDX engine.

A related option, ENABLE_SSON, is enabled by default.

If a security policy prevents you from enabling single sign-on on a device, configure Citrix Workspace app using Group Policy Object administrative template.

1. Open the Citrix Workspace app Group Policy Object administrative template by running gpedit.msc.
2. Choose **Administrative Templates** > **Citrix Components** > **Citrix Workspace** > **User authentication** > **Local user name and password**
3. Select **Enable pass-through authentication**.
4. Restart Citrix Workspace app for the changes to take effect.



© 1997–2026 Citrix Systems, Inc. All rights reserved.

To configure StoreFront:

When you configure the authentication service on the StoreFront server, select the Domain pass-through option. That setting enables Integrated Windows Authentication. You do not need to select the Smart card option unless you also have non domain-joined clients connecting to StoreFront using smart cards.

For more information about using smart cards with StoreFront, see Configure the authentication service in the StoreFront documentation.

Support for Conditional Access with Azure Active Directory

Conditional Access is a tool used by Azure Active Directory to enforce organizational policies. Workspace administrators can configure and enforce Azure Active Directory conditional access policies for users authenticating to the Citrix Workspace app. The Windows machine running the Citrix Workspace app must have Microsoft Edge WebView2 Runtime version 92 or later installed.

For complete details and instructions about configuring conditional access policies with Azure Active Directory, see Azure AD Conditional Access documentation.

> **Note:**
>
> This feature is supported only on Workspace (Cloud) deployments.

Other ways to authenticate to Citrix Workspace

You can configure the following authentication mechanisms with the Citrix Workspace app. For the following authentication mechanisms to work as expected, the Windows machine running the Citrix Workspace app must have Microsoft Edge WebView2 Runtime version 92 or later installed.

1. Windows Hello based authentication –For instructions about configuring Windows Hello based authentication, see Configure Windows Hello for Business Policy settings - Certificate Trust.

> **Note:**
>
> Windows Hello based authentication with domain pass-through is not supported.

1. FIDO2 Security Keys based authentication –FIDO2 security keys provide a seamless way for enterprise employees to authenticate without entering a user name or password. You can configure FIDO2 Security Keys based authentication to Citrix Workspace. If you would like your users to authenticate to Citrix Workspace with their Azure AD account using a FIDO2 security key, see Enable passwordless security key sign-in.
2. You can also configure Single Sign-On (SSO) to Citrix Workspace app from Microsoft Azure Active Directory (AAD) joined machines with AAD as an identity provider. For more details about

© 1997–2026 Citrix Systems, Inc. All rights reserved.

configuring Azure Active Directory Domain services, see Configuring Azure Active Directory Domain services. For information about how to connect Azure Active Directory to Citrix Cloud, see Connect Azure Active Directory to Citrix Cloud.

Smart card

Citrix Workspace app for Windows supports the following smart card authentication:

- **Pass-through authentication (single sign-on)** - Pass-through authentication captures the smart card credentials when users log on to Citrix Workspace app. Citrix Workspace app uses the captured credentials as follows:
  - Users of domain-joined devices who log on to Citrix Workspace app using the smart card can start virtual desktops and applications without needing to reauthenticate.
  - Citrix Workspace app running on non-domain joined devices with the smart card credentials must type their credentials again to start a virtual desktop or application.

  Pass-through authentication requires configuration both on StoreFront and Citrix Workspace app.
- **Bimodal authentication** - Bimodal authentication offers users a choice between using a smart card and typing the user name and password. This feature is effective when you can't use the smart card. For example, the logon certificate has expired. Dedicated stores must be set up per site to allow Bimodal authentication, using the **DisableCtrlAltDel** method set to **False** to allow smart cards. Bimodal authentication requires StoreFront configuration.

  Using the Bimodal authentication, the StoreFront administrator can allow both user name and password and smart card authentication to the same store by selecting them in the StoreFront console. See StoreFront documentation.
- **Multiple certificates** - Multiple certificates can be availed for a single smart card and if multiple smart cards are in use. When you insert a smart card in a card reader, the certificates are applicable to all applications running on the user device, including Citrix Workspace app.
- **Client certificate authentication** - Client certificate authentication requires Citrix Gateway and StoreFront configuration.
  - For access to StoreFront through Citrix Gateway, you must reauthenticate after removing the smart card.
  - When the Citrix Gateway SSL configuration is set to **Mandatory client certificate authentication**, operation is more secure. However, mandatory client certificate authentication isn't compatible with bimodal authentication.
- **Double hop sessions** - If a double-hop is required, a connection is established between Citrix Workspace app and the user's virtual desktop.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- **Smart card-enabled applications** - Smart card-enabled applications, such as Microsoft Outlook and Microsoft Office, allow users to digitally sign or encrypt documents available in virtual apps and desktops sessions.

Limitations:

- Certificates must be stored on the smart card and not on the user device.
- Citrix Workspace app does not save the choice of the user certificate, but stores the PIN when configured. The PIN is cached in non-paged memory only during the user session and isn't stored on the disk.
- Citrix Workspace app does not reconnect to a session when a smart card is inserted.
- When configured for smart card authentication, Citrix Workspace app does not support virtual private network (VPN) single-sign on or session pre-launch. To use VPN with smart card authentication, install the Citrix Gateway Plug-in. Log on through a webpage using their smart cards and PINs to authenticate at each step. Pass-through authentication to StoreFront with the Citrix Gateway Plug-in isn't available for smart card users.
- Citrix Workspace app updater communications with citrix.com and the Merchandising Server aren't compatible with smart card authentication on Citrix Gateway.

> **Warning**
>
> Some configuration requires registry edits. Using the Registry editor incorrectly might cause problems that can require you to reinstall the operating system. Citrix can't guarantee that problems resulting from incorrect use of the Registry Editor can be solved. Make sure you back up the registry before you edit it.

To enable single sign-on for smart card authentication:

To configure Citrix Workspace app for Windows, include the following command-line option during installation:

- `ENABLE_SSON=Yes`

  Single sign-on is another term for pass-through authentication. Enabling this setting prevents Citrix Workspace app from displaying a second prompt for a PIN.

- In the Registry editor, navigate to the following path and set the `SSONCheckEnabled` string to `False` if you have not installed the single sign-on component.

  `HKEY_CURRENT_USER\Software{ Wow6432 } \Citrix\AuthManager\protocols\integratedwindows\`

  `HKEY_LOCAL_MACHINE\Software{ Wow6432 } \Citrix\AuthManager\protocols\integratedwindows\`

  The key prevents the Citrix Workspace app authentication manager from checking for the single sign-on component and allows Citrix Workspace app to authenticate to StoreFront.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

To enable smart card authentication to StoreFront instead of Kerberos, install Citrix Workspace app for Windows with the following command-line options:

- `/includeSSON` installs single sign-on (pass-through) authentication. Enables credential caching and the use of pass-through domain-based authentication.
- If the user logs on to the endpoint with a different authentication method, for example, user name and password, the command line is:

  `/includeSSON LOGON_CREDENTIAL_CAPTURE_ENABLE=No`

This type of authentication prevents capturing of the credentials at logon time and allows Citrix Workspace app to store the PIN during Citrix Workspace app login.

1. Open the Citrix Workspace app Group Policy Object administrative template by running gpedit.msc.
2. Go to **Administrative Templates** > **Citrix Components** > **Citrix Workspace** > **User Authentication** > **Local user name and password**.
3. Select **Enable pass-through authentication**. Depending on the configuration and security settings, select **Allow pass-through authentication for all ICA option** for pass-through authentication to work.

To configure StoreFront:

- When you configure the authentication service, select the **Smart card** check box.

For more information about using smart cards with StoreFront, see Configure the authentication service in the StoreFront documentation.

To enable user devices for smart card use:

1. Import the certificate authority root certificate into the device's keystore.
2. Install your vendor's cryptographic middleware.
3. Install and configure Citrix Workspace app.

To change how certificates are selected:

By default, if multiple certificates are valid, Citrix Workspace app prompts the user to choose a certificate from the list. Instead, you can configure Citrix Workspace app to use the default certificate (per the smart card provider) or the certificate with the latest expiry date. If there are no valid logon certificates, the user is notified, and given the option to use an alternate logon method if available.

A valid certificate must have all of these characteristics:

- The current time of the clock on the local computer is within the certificate validity period.
- The **Subject public** key must use the RSA algorithm and have a key length of 1024 bits, 2048 bits, or 4096 bits.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- Key usage must include digital signature.
- Subject Alternative Name must include the User Principal Name (UPN).
- Enhanced key usage must include smart card logon and client authentication, or all key usages.
- One of the Certificate Authorities on the certificate's issuer chain must match one of the allowed Distinguished Names (DN) sent by the server in the TLS handshake.

Change how certificates are selected by using either of the following methods:

- On the Citrix Workspace app command line, specify the option `AM_CERTIFICATESELECTIONMODE={ Prompt | SmartCardDefault | LatestExpiry }`.

  Prompt is the default. For `SmartCardDefault` or `LatestExpiry`, if multiple certificates meet the criteria, Citrix Workspace app prompts the user to choose a certificate.

Add the following key value to the registry key `HKEY_CURRENT_USER OR HKEY_LOCAL_MACHINE\Software\[Wow6432Node\Citrix\AuthManager`: CertificateSelectionMode={ Prompt	SmartCardDefault	LatestExpiry }.

-

Values defined in `HKEY_CURRENT_USER` take precedence over values in `HKEY_LOCAL_MACHINE` to best assist the user in selecting a certificate.

To use CSP PIN prompts:

By default, the PIN prompts presented to users are provided by Citrix Workspace app for Windows rather than the smart card Cryptographic Service Provider (CSP). Citrix Workspace app prompts users to enter a PIN when required and then passes the PIN to the smart card CSP. If your site or smart card has more stringent security requirements, such as to disallow caching the PIN per-process or per-session, you can configure Citrix Workspace app to use the CSP components to manage the PIN entry, including the prompt for a PIN.

Change how PIN entry is handled by using either of the following methods:

- On the Citrix Workspace app command line, specify the option `AM_SMARTCARDPINENTRY=CSP`.
- Add the following key value to the registry key `HKEY_LOCAL_MACHINE\Software\[Wow6432Node\Citrix\AuthManager`: SmartCardPINEntry=CSP.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Smart card support and removal changes

A Citrix Virtual Apps session logs off when you remove the smart card. If Citrix Workspace app is configured with smart card as the authentication method, configure the corresponding policy on Citrix Workspace app for Windows to enforce the Citrix Virtual Apps session for logoff. The user is still logged into the Citrix Workspace app session.

Limitation:

When you log on to the Citrix Workspace app site using smart card authentication, the user name is displayed as **Logged On**.

Fast smart card Fast smart card is an improvement over the existing HDX PC/SC-based smart card redirection. It improves performance when smart cards are used in high-latency WAN environments.

Fast smart cards are supported on Windows VDA only.

To enable fast smart card logon on Citrix Workspace app:

Fast smart card logon is enabled by default on the VDA and disabled by default on Citrix Workspace app. To enable fast smart card logon, include the following parameter in the **`default.`**`ica` file of the associated StoreFront site:

```
copy[WFClient]
SmartCardCryptographicRedirection=On
```

To disable fast smart card logon on Citrix Workspace app:

To disable fast smart card logon on Citrix Workspace app, remove the `SmartCardCryptographicRedirecti` parameter from the **`default.`**`ica` file of the associated StoreFront site.

For more information, see smart-cards.

Silent authentication for Citrix Workspace

Citrix Workspace app introduces a Group Policy Object (GPO) policy to enable silent authentication for Citrix Workspace. This policy enables Citrix Workspace app to log in to Citrix Workspace automatically at system startup. Use this policy only when domain pass-through (single sign-on) is configured for Citrix Workspace on domain-joined devices.

For this policy to function, the following criteria must be met:

- Single sign-on must be enabled.
- The `SelfServiceMode` key must be set to `Off` in the Registry editor.

Enabling silent authentication:

© 1997–2026 Citrix Systems, Inc. All rights reserved.

1. Open the Citrix Workspace app Group Policy Object administrative template by running `gpedit.msc`.
2. Under the **Computer Configuration** node, go to **Administrative Templates** > **Citrix Workspace** > **Self Service**.
3. Click the **Silent authentication for Citrix Workspace** policy and set it to **Enabled**.
4. Click **Apply** and **OK**.

Secure communications

September 7, 2025

To secure the communication between Citrix Virtual Apps and Desktops server and Citrix Workspace app, you can integrate your Citrix Workspace app connections using a range of secure technologies such as the following:

- Citrix Gateway: For information, see the topics in this section and the Citrix Gateway, and StoreFront documentation.
- A firewall: Network firewalls can allow or block packets based on the destination address and port.
- Transport Layer Security (TLS) versions 1.0 through 1.2 are supported.
- Trusted server to establish trust relations in Citrix Workspace app connections.
- ICA® file signing
- Local Security Authority (LSA) protection
- Proxy server for Citrix Virtual Apps deployments only: A SOCKS proxy server or secure proxy server. Proxy servers help to limit access to and from the network. They also handle the connections between Citrix Workspace app and the server. Citrix Workspace app supports SOCKS and secure proxy protocols.
- Outbound proxy

Citrix Gateway

Citrix Gateway (formerly Access Gateway) secures connections to StoreFront stores. Also, lets administrators control user access to desktops and applications in a detailed way.

To connect to desktops and applications through Citrix Gateway:

1. Specify the Citrix Gateway URL that your administrator provides using one of the following ways:

    - The first time you use the self-service user interface, you are prompted to enter the URL in the **Add Account** dialog box.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- When you later use the self-service user interface, enter the URL by clicking **Preferences** > **Accounts** > **Add**.
- If you're establishing a connection with the storebrowse command, enter the URL at the command line

The URL specifies the gateway and, optionally, a specific store:

- To connect to the first store that Citrix Workspace app finds, use a URL in the following format:
  - https://gateway.company.com
- To connect to a specific store, use a URL of the form, for example: https://gateway.company.com?<storename>. This dynamic URL is in a non-standard form; do not include "="(the "equals"sign character) in the URL. If you're establishing a connection to a specific store with storebrowse, you might need quotation marks around the URL in the storebrowse command.

1. When prompted, connect to the store (through the gateway) using your user name, password, and security token. For more information about this step, see the Citrix Gateway documentation.

When authentication is complete, your desktops and applications are displayed.

Connecting through firewall

Network firewalls can allow or block packets based on the destination address and port. If you're using a firewall, Citrix Workspace app for Windows can communicate through the firewall with both the Web server and the Citrix server.

Common Citrix Communication Ports

Source	Type	Port	Details
Citrix Workspace app	TCP	80/443	Communication with StoreFront
ICA or HDX	TCP/UDP	1494	Access to applications and virtual desktops
ICA or HDX with Session Reliability	TCP/UDP	2598	Access to applications and virtual desktops
ICA or HDX over TLS	TCP/UDP	443	Access to applications and virtual desktops

For more information about the ports, see the Knowledge Center article CTX101810.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Transport Layer Security

Transport Layer Security (TLS) is the replacement for the SSL (Secure Sockets Layer) protocol. The Internet Engineering Taskforce (IETF) renamed it TLS when it took over responsibility for the development of TLS as an open standard.

TLS secures data communications by providing server authentication, encryption of the data stream, and message integrity checks. Some organizations, including U.S. government organizations, require the use of TLS to secure data communications. These organizations might also require the use of validated cryptography, such as Federal Information Processing Standard (FIPS) 140. FIPS 140 is a standard for cryptography.

To use TLS encryption as the communication medium, you must configure the user device and the Citrix Workspace app. For information about securing StoreFront communications, see the Secure section in the StoreFront documentation. For information about securing VDA, see Transport Layer Security (TLS) in the Citrix Virtual Apps and Desktops documentation.

You can use the following policies to:

- Enforce use of TLS: We recommend that you use TLS for connections using untrusted networks, including the Internet.
- Enforce use of FIPS (Federal Information Processing Standards): Approved cryptography and follow the recommendations in NIST SP 800-52. These options are disabled by default.
- Enforce use of a specific version of TLS and specific TLS cipher suites: Citrix supports the TLS 1.0, TLS 1.1, and TLS 1.2 protocols.
- Connect only to specific servers.
- Check for revocation of the server certificate.
- Check for a specific server-certificate issuance policy.
- Select a particular client certificate, if the server is configured to request one.

Citrix Workspace app for Windows supports the following cipher suites for TLS 1.2 protocol:

- TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384
- TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384
- TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA

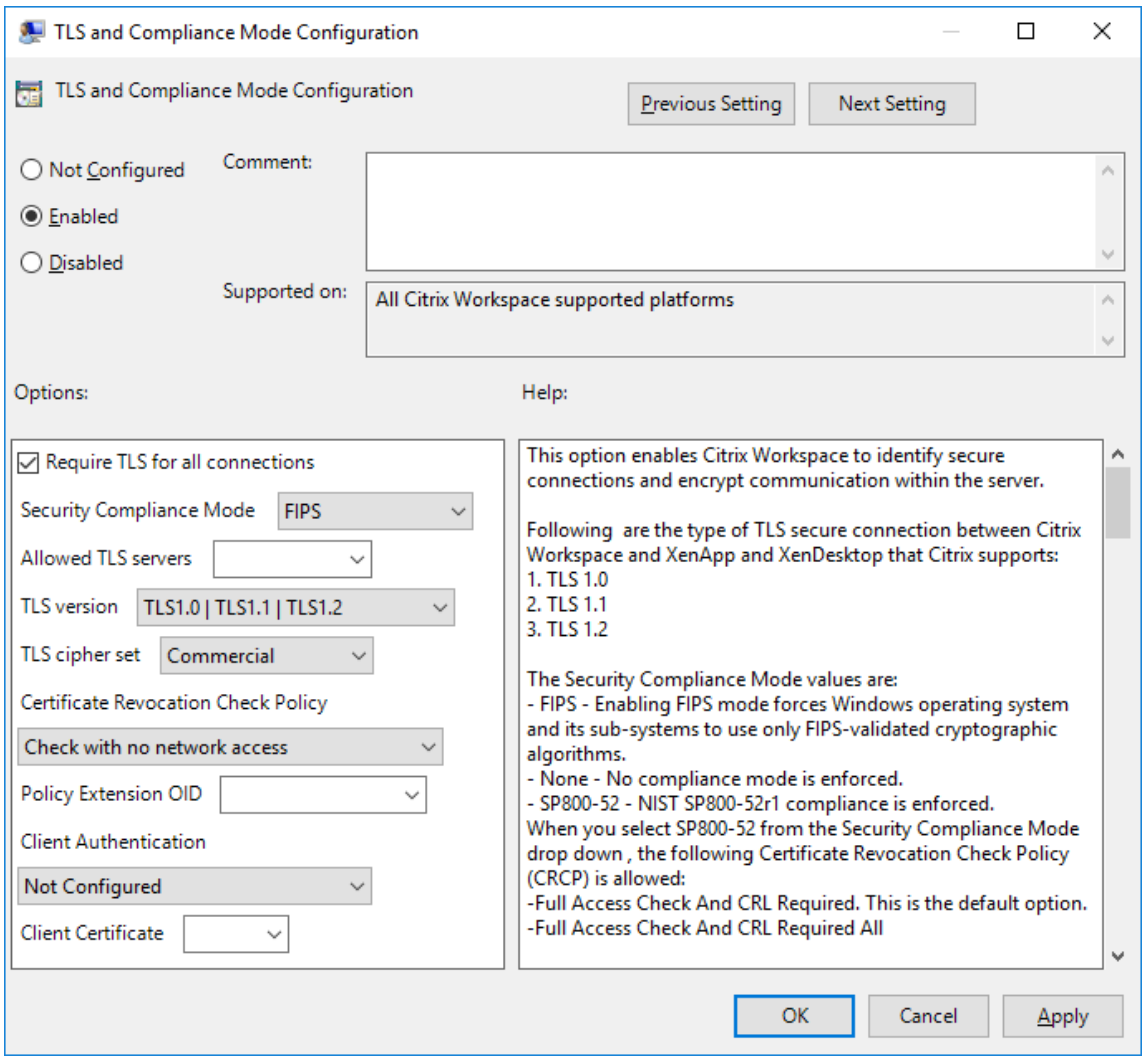
> **Important:**
>
> The following cipher suites are deprecated for enhanced security:
>
> - Cipher suites RC4 and 3DES
> - Cipher suites with prefix "TLS_RSA_*"
> - TLS_RSA_WITH_AES_256_GCM_SHA384 (0x009d)
> - TLS_RSA_WITH_AES_128_GCM_SHA256 (0x009c)

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- TLS_RSA_WITH_AES_256_CBC_SHA256 (0x003d)
- TLS_RSA_WITH_AES_256_CBC_SHA (0x0035)
- TLS_RSA_WITH_AES_128_CBC_SHA (0x002f)
- TLS_RSA_WITH_RC4_128_SHA (0x0005)
- TLS_RSA_WITH_3DES_EDE_CBC_SHA (0x000a)

TLS support

1. Open the Citrix Workspace app GPO administrative template by running gpedit.msc.
2. Under the **Computer Configuration** node, go to **Administrative Templates** > **Citrix Workspace** > **Network routing**, and select the **TLS and Compliance Mode Configuration** policy.



3. Select **Enabled** to enable secure connections and to encrypt communication on the server. Set the following options:

© 1997–2026 Citrix Systems, Inc. All rights reserved.

> **Note:**
>
> Citrix recommends TLS for secure connections.

a) Select **Require TLS for all connections** to force Citrix Workspace app to use TLS for connections to published applications and desktops.

b) From the **Security Compliance Mode** menu, select the appropriate option:

   i. **None** - No compliance mode is enforced.
   ii. **SP800-52** - Select **SP800-52** for compliance with NIST SP 800-52. Select this option only if the servers or gateway follow NIST SP 800-52 recommendations.

   > **Note:**
   >
   > If you select **SP800-52**, FIPS Approved cryptography is automatically used, even if **Enable FIPS** isn't selected. Also, enable the Windows security option, **System Cryptography: Use FIPS-compliant algorithms for encryption, hashing, and signing**. Otherwise, Citrix Workspace app might fail to connect to the published applications and desktops.

   If you select **SP800-52**, set the **Certificate Revocation Check Policy** setting to **Full access check and CRL required**.

   When you select **SP800-52**, Citrix Workspace app verifies that the server certificate follows the recommendations in NIST SP 800-52. If the server certificate does not comply, Citrix Workspace app might fail to connect.

   i. **Enable FIPS** - Select this option to enforce the use of FIPS approved cryptography. Also, enable the Windows security option from the operating system group policy, **System Cryptography: Use FIPS-compliant algorithms for encryption, hashing, and signing**. Otherwise, Citrix Workspace app might fail to connect to published applications and desktops.

c) From the **Allowed TLS servers** drop-down menu, select the port number. Use a comma-separated list to ensure that the Citrix Workspace app connects only to a specified server. You can specify wildcards and port numbers. For example, *.citrix.com: 4433 allows connections to any server whose common name ends with .citrix.com on port 4433. The issuer of the certificate asserts the accuracy of the information in a security certificate. If Citrix Workspace does not recognize or trust the issuer, the connection is rejected.

d) From the **TLS version** menu, select one of the following options:

- **TLS 1.0, TLS 1.1, or TLS 1.2** - This is the default setting. This option is recommended only if there is a business requirement for TLS 1.0 for compatibility.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- **TLS 1.1 or TLS 1.2** - Use this option to ensure that the connections use either TLS 1.1 or TLS 1.2.
- **TLS 1.2** - This option is recommended if TLS 1.2 is a business requirement.

a) **TLS cipher set** - To enforce use of a specific TLS cipher set, select Government (GOV), Commercial (COM), or All (ALL).

b) From the **Certificate Revocation Check Policy** menu, select any of the following:

- **Check with No Network Access** - Certificate Revocation list check is done. Only local certificate revocation list stores are used. All distribution points are ignored. A Certificate Revocation List check that verifies the server certificate available from the target SSL Relay/Citrix Secure Web Gateway server isn't mandatory.
- **Full Access Check** - Certificate Revocation List check is done. Local Certificate Revocation List stores and all distribution points are used. If revocation information for a certificate is found, the connection is rejected. Certificate Revocation List check for verifying the server certificate available from the target server isn't critical.
- **Full Access Check and CRL Required** - Certificate Revocation List check is done, except for the root Certificate Authority. Local Certificate Revocation List stores and all distribution points are used. If revocation information for a certificate is found, the connection is rejected. Finding all required Certificate Revocation Lists is critical for verification.
- **Full Access Check and CRL Required All** - Certificate Revocation List check is done, including the root CA. Local Certificate Revocation List stores and all distribution points are used. If revocation information for a certificate is found, the connection is rejected. Finding all required Certificate Revocation Lists is critical for verification.
- **No Check** - No Certificate Revocation List check is done.

a) Using the **Policy Extension OID**, you can limit Citrix Workspace app to connect only to servers with a specific certificate issuance policy. When you select **Policy Extension OID**, Citrix Workspace app accepts only server certificates that contain the Policy Extension OID.

b) From the **Client Authentication** menu, select any of the following:

- **Disabled** - Client Authentication is disabled.
- **Display certificate selector** - Always prompt the user to select a certificate.
- **Select automatically if possible** - Prompt the user only if there a choice of the certificate to identify.
- **Not configured** - Indicates that client authentication isn't configured.
- **Use specified certificate** - Use the client certificate as set in the Client Certificate option.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

a) Use the **Client Certificate** setting to specify the identifying certificate's thumbprint to avoid prompting the user unnecessarily.

b) Click **Apply** and **OK** to save the policy.

Trusted server

Trusted server configuration identifies and enforces trust relations in Citrix Workspace app connections.

When you enable Trusted server, Citrix Workspace app specifies the requirements and decides if the connection to the server can be trusted. For example, a Citrix Workspace app connecting to a certain address, such as `https://\*.citrix.com` with a specific connection type (such as TLS) is directed to a trusted zone on the server.

When you enable this feature, the connected server is in the Windows **Trusted Sites zone**. For instructions about adding servers to the Windows **Trusted Sites zone**, see the Internet Explorer online help.

To enable trusted server configuration using Group Policy Object administrative template

Prerequisite:

Exit from the Citrix Workspace app components including the Connection Center.

1. Open the Citrix Workspace app GPO administrative template by running gpedit.msc.
2. Under the **Computer Configuration** node, go to **Administrative Templates** > **Citrix Components** > **Citrix Workspace** > **Network Routing** > **Configure trusted server configuration**.
3. Select **Enabled** to force Citrix Workspace app for region identification.
4. Select **Enforce trusted server configuration**. This option forces the client to perform the identification using a trusted server.
5. From the **Windows internet zone** drop-down menu, select the client-server address. This setting is applicable only to the Windows Trusted Site zone.
6. In the **Address** field, set the client-server address for the trusted site zone other than the Windows. You can use a comma-separated list.
7. Click **OK** and **Apply**.

ICA file signing

The ICA file signing helps protect you from an unauthorized application or desktop launch. Citrix Workspace app verifies that a trusted source generated the application or desktop launch based on an administrative policy and protects against launches from untrusted servers. You can configure ICA file signing using the Group policy objects administrative template or StoreFront. The ICA file signing feature isn't enabled by default.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

For information about enabling ICA file signing for StoreFront, see Enable ICA file signing in StoreFront documentation.

Configure ICA file signature

> **Note:**
>
> If the CitrixBase.admx\adml isn't added to the local GPO, the **Enable ICA File Signing** policy might not be present.

1. Open the Citrix Workspace app Group Policy Object administrative template by running gpedit.msc
2. Under the **Computer Configuration** node, go to **Administrative Templates** > **Citrix Components**.
3. Select **Enable ICA File Signing** policy and select one of the options as required:
    a) Enabled - Indicates that you can add the signing certificate thumbprint to the allow list of trusted certificate thumbprints.
    b) Trust Certificates - Click **Show** to remove the existing signing certificate thumbprint from the allow list. You can copy and paste the signing certificate thumbprints from the signing certificate properties.
    c) Security policy - Select one of the following options from the menu.
        i. Only allow signed launches (more secure): Allows only signed application and desktop launches from a trusted server. A security warning appears when there's an invalid signature. The session launch fails because of non-authorization.
        ii. Prompt user on unsigned launches (less secure) - A message prompt appears when an unsigned or invalidly signed session is launched. You can choose to either continue the launch or cancel the launch (default).
4. Click **Apply** and **OK** to save the policy.
5. Restart the Citrix Workspace app session for the changes to take effect.

To select and distribute a digital signature certificate:

When selecting a digital signature certificate, we recommend you choose from the following priority list:

1. Buy a code-signing certificate or SSL signing certificate from a public Certificate Authority (CA).
2. If your enterprise has a private CA, create a code-signing certificate or SSL signing certificate using the private CA.
3. Use an existing SSL certificate.
4. Create a root CA certificate and distribute it to user devices using GPO or manual installation.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Local Security Authority (LSA) protection

Citrix Workspace app supports Windows Local Security Authority (LSA) protection, which maintains information about all aspects of local security on a system. This support provides the LSA level of system protection to hosted desktops.

Connecting through proxy server

Proxy servers are used to limit access to and from your network, and to handle connections between Citrix Workspace app for Windows and servers. Citrix Workspace app supports SOCKS and secure proxy protocols.

When communicating with the server, Citrix Workspace app uses proxy server settings that are configured remotely on the server running workspace for web.

When communicating with the web server, Citrix Workspace app uses the proxy server settings configured through the **Internet** settings of the default web browser on the user device. Configure the **Internet** settings of the default web browser on the user device accordingly.

To enforce proxy settings through the ICA file on StoreFront, see Citrix Knowledge Center article CTX136516.

Outbound proxy support

SmartControl allows administrators to configure and enforce policies that affect the environment. For instance, you might want to prohibit users from mapping drives to their remote desktops. You can achieve the granularity using the SmartControl feature on the Citrix Gateway.

The scenario changes when the Citrix Workspace app and the Citrix Gateway belong to separate enterprise accounts. In such cases, the client domain can't apply the SmartControl feature because the gateway doesn't exist on the domain. You can then use the Outbound ICA Proxy. The Outbound ICA Proxy feature lets you use the SmartControl feature even when Citrix Workspace app and Citrix Gateway are deployed in different organizations.

Citrix Workspace app supports session launches using the NetScaler LAN proxy. Use the outbound proxy plug-in to configure a single static proxy or select a proxy server at runtime.

You can configure outbound proxies using the following methods:

- Static proxy: Proxy server is configured by giving a proxy host name and port number.
- Dynamic proxy: A single proxy server can be selected among one or more proxy servers using the proxy plug-in DLL.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

You can configure the outbound proxy using the Group Policy Object administrative template or the Registry editor.

For more information about outbound proxy, see Outbound ICA Proxy support in the Citrix Gateway documentation.

Outbound proxy support - Configuration

> **Note:**
>
> If both static proxy and dynamic proxies are configured, the dynamic proxy configuration takes precedence.

Configuring the outbound proxy using the GPO administrative template:

1. Open the Citrix Workspace app Group Policy Object administrative template by running gpedit.msc.
2. Under the **Computer Configuration** node, go to **Administrative Templates** > **Citrix Workspace** > **Network routing**.
3. Select one of the following options:
   - For static proxy: Select the **Configure NetScaler® LAN proxy manually** policy. Select **Enabled** and then provide the host name and port number.
   - For dynamic proxy: Select the **Configure NetScaler LAN proxy using DLL** policy. Select **Enabled** and then provide the full path to the DLL file. For example, `C:\Workspace\Proxy\ProxyChooser.dll`.
4. Click **Apply** and **OK**.

Configuring the outbound proxy using the Registry editor:

- **For static proxy:**
  - Launch the Registry editor and navigate to `HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Citrix\ICA Client\Engine\Network Routing\Proxy\NetScaler`.
  - Create DWORD value keys as follows:

    ```
    "StaticProxyEnabled"=dword:00000001
    "ProxyHost"="testproxy1.testdomain.com
    "ProxyPort"=dword:000001bb
    ```

- **For dynamic proxy:**

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- Launch the Registry editor and navigate to `HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Citrix\ICA Client\Engine\Network Routing\Proxy\NetScaler LAN Proxy`.
- Create DWORD value keys as follows:

```
"DynamicProxyEnabled"=dword:00000001
"ProxyChooserDLL"="c:\\Workspace\\Proxy\\ProxyChooser.dll"
```

Storebrowse

September 7, 2025

Storebrowse is a command-line utility that interacts between the client and the server. It's used to authenticate all the operations within StoreFront and with Citrix Gateway.

Using the **Storebrowse** utility, administrators can automate the following operations:

- Add a store.
- List the published apps and desktops from a configured store.
- Generate an ICA® file by selecting any published virtual apps and desktops manually.
- Generate an ICA file using the **Storebrowse** command line.
- Launch the published application.

The **Storebrowse** utility is a part of the `Authmanager` component. When Citrix Workspace app installation is complete, the **Storebrowse** utility is in the `AuthManager` installation folder.

To confirm that the **Storebrowse** utility is installed along with the `Authmanager` component, check the following registry path:

When Citrix Workspace app is installed by administrators:

On a 32-bit machine	[HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\AuthManager\Inst
On a 64-bit machine	[HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\Citrix\A

When Citrix Workspace app is installed by users (non-administrators):

On a 32-bit machine	[HKEY_CURRENT_USER\SOFTWARE\Citrix\AuthManager\Insta

© 1997–2026 Citrix Systems, Inc. All rights reserved.

On a 64-bit machine	[HKEY_CURRENT_USER\SOFTWARE\WOW6432Node\Citrix\Au

Requirements

- Citrix Workspace app Version 1808 for Windows or later.
- Minimum of 530 MB of free disk space.
- 2 GB RAM.

Compatibility Matrix

Storebrowse utility is compatible with the following operating systems:

Operating system
Windows 10 32-bit and 64-bit editions
Windows 8.1, 32-bit and 64-bit editions
Windows 7 SP1, 32-bit and 64-bit editions
Windows Thin PC
Windows Server 2016
Windows Server 2012 R2, Standard, and, Data center editions
Windows Server 2012, Standard, and, Data center editions
Windows Server 2008 R2, 64-bit edition
Windows Server 2008 R2, 64-bit edition

Connections

Storebrowse utility supports the following types of connections:

- HTTP store
- HTTPS store
- Citrix Gateway 11.0 and later

© 1997–2026 Citrix Systems, Inc. All rights reserved.

> **Note:**
>
> On an HTTP store, the **Storebrowse** utility does not accept credentials using the command-line.

Authentication methods

StoreFront servers StoreFront supports different authentication methods to access stores, however, not all are recommended. For security purposes, some of the authentication methods are disabled by default while creating a store.

- **Username and Password**: Enter the credentials to be authenticated to access stores. By default, Explicit authentication is enabled when you create your first store.
- **Domain Pass-through**: After authenticating to the domain-joined Windows computers, you're automatically signed in to stores. To use this option, enable pass-through authentication when installing the Citrix Workspace app. For more information on domain pass-through, see Configuring Pass-through authentication.
- **HTTP Basic**: Enable HTTP Basic authentication so that the **Storebrowse** utility can communicate with the StoreFront servers. This option is disabled by default on the StoreFront server. Enable the **HTTP Basic authentication** method.

Storebrowse utility supports authentication methods in any of the following methods:

- Using the `AuthManager` that is in-built along with the **Storebrowse** utility. Note: Enable the HTTP Basic authentication method on the StoreFront while working with the **Storebrowse** utility. This applies when the user provides the credentials using the **Storebrowse** commands.
- External `Authmanager` that can be included with Citrix Workspace app for Windows.

Single sign-on with Citrix Gateway

In addition to the newly added Citrix Gateway support, you can now use single sign-on with it. You can add a store and list the published resources without having to provide your user credentials.

For more information about single sign-on support with Citrix Gateway, see Support for single sign-on with Citrix Gateway.

> **Note:**
>
> This feature is supported only on domain-joined machines where the Citrix Gateway is configured with the single sign-on authentication.

Launch published desktop or application

You can now launch a resource directly from the store without having to use an ICA file.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Command usage

The following section provides detailed information about the commands that you can use from the **Storebrowse** utility.

`-a, --addstore`

Description:

Adds new store. Returns the full URL of the store. If the return fails, an error is reported.

> **Note:**
>
> Multi-store configuration is supported on the **Storebrowse** utility.

Command example on StoreFront:

Command:

```
storebrowse.exe –U *username* -P *password* -D *domain* -a *URL of StoreFront*
```

Example:

```
.\storebrowse.exe –U { Username } –P { Password } –D { Domain } –a [https://my.firstexamplestore.net](https://my.firstexamplestore.net)
```

Command example on Citrix Gateway:

Command:

```
storebrowse.exe –U *username* -P *password* -D *domain* -a *URL of CitrixGateway*
```

Example:

```
.\storebrowse.exe –U { Username } –P { Password } –D { Domain } –a <https://mysecondexample.com>
```

`/?`

Description:

Provides details on **Storebrowse** utility usage.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

(-l),--liststore

Description:

Lists the stores that are added by the user.

Command Example on StoreFront:

```
.\storebrowse.exe –l
```

Command Example on Citrix Gateway:

```
.\storebrowse.exe –l
```

(-M 0x2000 -E)

Description:

Enumerates resources.

Command example on StoreFront:

```
.\storebrowse.exe –U { Username } –P { Password } –D { Domain } –M 0
x2000 –E <https://my.firstexamplestore.net/Citrix/Store/discovery>
```

Command example on Citrix Gateway:

```
.\storebrowse.exe –U { Username } –P { Password } –D { Domain } –M 0
x2000 –E <https://my.secondexample.net>
```

-q,--quicklaunch

Description:

Generates the ICA file for published apps and desktops using the **Storebrowse** utility. The `quicklaunch` option requires a launch URL as an input along with the Store URL. The launch URL which can either be the StoreFront server or the Citrix Gateway URL. The ICA file is generated in the `%LocalAppData%\Citrix\Storebrowse\cache` directory.

You can get the launch URL for any published apps and desktops by running the following command:

```
.\storebrowse –M 0X2000 –E https://myfirstexamplestore.net/Citrix/
Second/discovery
```

A typical launch URL is as follows:

```
'Controller.Calculator''Calculator''\' ''http://abc-sf.xyz.com/Citrix
/Stress/resources/v2/Q29udHJvbGxlci5DYWxjdWxhdG9y/launch/ica
```

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Command example on StoreFront:

```
.\storebrowse.exe –U { Username } –P { Password } –D { Domain } –q {
Launch_URL_of_published_ apps and desktops } <https://my.firstexamplestore
.net/Citrix/Store/resources/v2/Q2hJkOlmNoPQrSTV9y/launch/ica> <https
://my.firstexamplestore.net/Citrix/Store/discovery>
```

Command example on Citrix Gateway:

```
.\storebrowse.exe –U { Username } –P { Password } –D { Domain } –q {
Launch_URL_of_published_ apps and desktops } <https://my.secondexmaplestore
.com>
```

-L, --launch

Description:

Generates the required ICA file for published apps and desktops using the **Storebrowse** utility. The launch option requires the name of the resource along with the Store URL. The name which can either be the StoreFront server or the Citrix Gateway URL. The ICA file is generated in the `%LocalAppData%\Citrix\Storebrowse\cache` directory.

Run the following command to get the display name of the published apps and desktops:

```
.\storebrowse –M 0X2000 –E https://myfirstexamplestore.net/Citrix/
Second/discovery
```

This command results in the following output:

```
'Controller.Calculator''Calculator''\' ''http://abc-sf.xyz.com/Citrix
/Stress/resources/v2/Q29udHJvbGxlci5DYWxjdWxhdG9y/launch/ica
```

Command example on StoreFront:

```
.\storebrowse.exe -U { Username } –P { Password } –D { Domain } –L
“{ Resource_Name } <https://my.firstexamplestore.net/Citrix/Store/
discovery>
```

Command example on Citrix Gateway:

```
<.\storebrowse.exe –U { Username } –P { Password } –D { Domain } –L {
Resource_Name } https://my.secondexamplestore.com>
```

-S, --sessionlaunch

Description:

© 1997–2026 Citrix Systems, Inc. All rights reserved.

With this command, you can add a store, verify, and launch the published resources. This option takes the following as parameters:

- User name
- Password
- Domain
- Name of the resource to be launched
- Store URL

However, if the user does not provide the credentials, the AuthManager prompts to enter the credentials and then the resource is launched.

You can get the name of the resource of published apps and desktops by running the following command:

```
.\storebrowse –M 0X2000 –E https://myfirstexamplestore.net/Citrix/Second/discovery
```

This command results in the following output:

```
'Controller.Calculator''Calculator''\' ''http://abc-sf.xyz.com/Citrix/Stress/resources/v2/Q29udHJvbGxlci5DYWxjdWxhdG9y/launch/ica
```

The name that is in bold in the previous output is used as the input parameter to the –S option.

Command example on StoreFront:

```
.\storebrowse.exe -U { Username } –P { Password } –D { Domain } –S “{ Friendly_Resource_Name } <https://my.firstexamplestore.net/Citrix/Store/discovery >
```

Command example on Citrix Gateway:

```
.\storebrowse.exe –U { Username } –P { Password } –D { Domain } –S { Friendly_Resource_Name } <https://my.secondexamplestore.com>
```

-f, --filefolder

Description:

Generates the ICA file in the custom path for the published apps and desktops.

The launch option requires a folder name and the name of the resource as the input with the Store URL. The Store URL can either be the StoreFront server or the Citrix Gateway URL.

Command example on StoreFront:

```
.\storebrowse.exe –f “C:\Temp\Launch.ica” –L “Resource_Name” { Store }
```

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Command example on the Citrix Gateway:

```
.\storebrowse.exe –f “C:\Temp\Launch.ica” –L “Resource_Name” { NSG_URL
 }
```

-t, --traceauthentication

Description:

Generates logs for the AuthManager component. Logs are generated only if the **Storebrowse** utility is using an in-built AuthManager. Logs are generated in the localappdata%\Citrix\Storebrowse\logs directory.

> **Note:**
>
> This option must not be the last parameter listed in the user’s command line.

Command example on StoreFront:

```
.\storebrowse.exe –t –U { UserName } –P { Password } –D { Domain } –a
{ StoreURL }
```

Command example on Citrix Gateway:

```
.\storebrowse.exe –t –U { UserName } –P { Password } –D { Domain } –a
{ NSG_URL }
```

-d, --deletestore

Description:

Deletes existing StoreFront or Citrix Gateway store.

Command example on StoreFront:

```
.\storebrowse.exe –d https://my.firstexamplestore.net/Citrix/Store/
discovery
```

Command example on Citrix Gateway:

```
.\storebrowse.exe –d https://my.secondexmaplestore.com
```

Single sign-on support with Citrix Gateway

Single sign-on lets you authenticate to a domain and use the Citrix Virtual Apps and Desktops™ and Citrix DaaS (formerly Citrix Virtual Apps and Desktops service)that the domain provides. You can sign

© 1997–2026 Citrix Systems, Inc. All rights reserved.

in without having to reauthenticate to each app or desktop. When you add a store, your credentials pass through the Citrix Gateway server, along with the Citrix Virtual Apps and Desktops and Citrix DaaS, and Start menu settings.

This feature is supported on Citrix Gateway Version 11 and later.

Prerequisites:

For the prerequisites on how to configure Single Sign-On for the Citrix Gateway, see Configure domain pass-through authentication.

The single sign-on feature with Citrix Gateway can be enabled using the Group Policy Object (GPO) administrative template.

1. Open the Citrix Workspace app GPO administrative template by running gpedit.msc
2. Under the **Computer Configuration node**, go to **Administrative Template** > **Citrix Component** > **Citrix Workspace** > **User Authentication** > **Single Sign-on for Citrix Gateway**.
3. Use the toggle options to Enable or Disable the Single Sign-On option.
4. Click **Apply** and **OK**.
5. Restart the Citrix Workspace app session for the changes to take effect.

Limitations:

- Enable the **HTTP Basic Authentication** method on the StoreFront server for credential injection operations with the **Storebrowse** utility.
- If you have an HTTP store and try to connect to the store using the utility to check or launch the published virtual apps and desktops, the credential injection using the command-line option is unsupported. As a workaround, use the external `AuthManager` module if you do not provide credential using the command line.
- **Storebrowse** utility currently supports only single store configured the Citrix Gateway on the StoreFront server.
- Credential Injection in the **Storebrowse** utility works only if the Citrix Gateway is configured with Single-Factor Authentication.
- The command-line options `Username (-U)`, `Password (-P)` and `Domain (-D)` of the **Storebrowse** utility are case-sensitive and must be in upper case only.

To enable SSON for third-party applications that uses ICOSDK, create the following registry:

- Registry Key: `Computer\HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\Citrix\ICA Client\NonIEAppsWithSson`
- Registry Value: full path of the third-party applications
- Registry Type: reg_multi_sz

Example:

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- Registry Key: `Computer\HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\Citrix\ICA Client\NonIEAppsWithSson`
- Registry Value: C:\temp1\abc.exe;C:\temp2\xyz.exe
- Registry Type: reg_multi_sz

> **Note:**
>
> - You can provide multiple third-party applications separated by semicolon.

Citrix Workspace app Desktop Lock

September 7, 2025

You can use the Citrix Workspace app Desktop Lock when you do not need to interact with the local desktop. You can use the Desktop Viewer (if enabled), however it has only the following set of options on the toolbar:

- Ctrl+Alt+Del
- Preferences
- Devices
- Disconnect.

Citrix Workspace app for Windows with Desktop Lock works on domain-joined machines that are single sign-on enabled and store configured. It doesn't support PNA sites. Previous versions of Desktop Lock aren't supported when you upgrade to Citrix Receiver for Windows 4.2 or later.

Install Citrix Workspace app for Windows with the `/includeSSON` flag. Configure the store and single sign-on, either using the adm/admx file or command line option. For more information, see Install.

Then, install the Citrix Workspace app Desktop Lock as an administrator using the `CitrixWorkspaceDesktopL` `.msi` available in the Citrix Downloads page.

System requirements

- Microsoft Visual C++ 2005 Service Pack 1 Redistributable Package. For more information, see the Microsoft Download page.
- Supported on Windows 8, and Windows 8.1, Windows 10 (Anniversary update included), and Windows 11.
- Connects to StoreFront through native protocols only.
- Domain-joined end points.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- User devices must be connected to a LAN or WAN.

Local App Access

> **Important**
>
> Enabling Local App Access might allow local desktop access unless a full lockdown has been applied with the Group Policy Object template or a similar policy. For more information, see the Configure Local App Access and URL redirection section in the Citrix Virtual Apps and Desktops documentation.

Working with Citrix Workspace app Desktop Lock

- You can use Citrix Workspace app Desktop Lock with the following Citrix Workspace app features:
  - 3Dpro, Flash, USB, HDX™ Insight, Microsoft Lync 2013 plug-in, and Local App Access
  - Domain, two-factor authentication, or smart card authentication only
- Disconnecting the Citrix Workspace app Desktop Lock session logs out the end device.
- Flash redirection is disabled on Windows 8 and later versions. Flash redirection is enabled on Windows 7.
- The Desktop Viewer is optimized for Citrix Workspace app Desktop Lock with no Home, Restore, Maximize, and Display properties.
- Ctrl+Alt+Del is available on the Desktop Viewer toolbar.
- Most windows shortcut keys are passed to the remote session, except for Windows+L.
- Ctrl+F1 triggers Ctrl+Alt+Del when you disable the connection or Desktop Viewer for desktop connections.

> **Note:**
>
> With the Desktop Lock installed, and `LiveInDesktopDisconnectOnLock` set to **False** in the registry path `HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\Dazzle` Or `HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Citrix\Dazzle`, the active session gets disconnected when the end-point wakes up from hibernation or standby mode.

Install Citrix Workspace app Desktop Lock

This procedure installs Citrix Workspace app for Windows so that virtual desktops appear using Citrix Workspace app Desktop Lock. For deployments that use smart cards, see Smart card.

1. Sign in using a local administrator account.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

2. At a command prompt, run the following command:

   For example:

   ```
   CitrixWorkspaceApp.exe
        /includeSSON
   STORE0="DesktopStore;https://my.storefront.server/Citrix/MyStore/
      discovery;on;Desktop Store"
   ```

   The command is available in the Citrix Workspace app and **Plug-ins** > **Windows** > **Citrix Workspace app** folder on the installation media. For command details, see the Citrix Workspace app install documentation at Install.

3. In the same folder on the installation media, double-click `CitrixWorkspaceDesktopLock.msi`. The Desktop Lock wizard appears. Follow the prompts.

4. When the installation completes, restart the user device. If you have permission to access a desktop and you sign in as a domain user, the device appears using Citrix Workspace app Desktop Lock.

You can allow administration of the user device after installation, the account used to install `CitrixWorkspaceDesktopLock.msi` is excluded from the replacement shell. If that account is later deleted, you can't sign in and administer the device.

To run a **silent install** of Citrix Workspace Desktop Lock, use the following command line:

```
msiexec /i CitrixWorkspaceDesktopLock.msi /qn
```

Configure Citrix Workspace app Desktop Lock

When you've signed in as a non-administrator, Desktop Lock automatically launches an assigned desktop session.

Using Active Directory policies prevent users from hibernating virtual desktops.

Use the same administrator account to configure Citrix Workspace app Desktop Lock as you did to install it.

- Check if the receiver.admx (or receiver.adml) and receiver_usb.admx (.adml) files are loaded into Group Policy (where the policies appear in Computer Configuration or **User Configuration** > **Administrative Templates** > **Classic Administrative Templates (ADMX)** > **Citrix Components**). The .admx files are in %Program Files%\Citrix\ICA Client\Configuration\.
- USB preferences - When a user plugs in a USB device, that device is automatically remoted to the virtual desktop and no user interaction is required. The virtual desktop controls the USB device and displaying it in the user interface.
    - Enable the USB policy rule.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

    - In **Citrix Workspace app** > **Remoting client devices** > **Generic USB Remoting**, enable and configure the Existing USB Devices and New USB Devices policies.

- Drive mapping - In **Citrix Workspace app** > **Remoting client devices**, enable and configure the Client drive mapping policy.
- Microphone - In **Citrix Workspace app** > **Remoting client devices**, enable and configure the Client microphone policy.

Configure smart cards for use with Windows Desktop Lock

1. Configure StoreFront.
    a) Configure the XML Service to use DNS Address Resolution for Kerberos support.
    b) Configure StoreFront sites for HTTPS access, create a server certificate signed by your domain certificate authority, and add HTTPS binding to the default website.
    c) Make sure that pass-through authentication with the smart card is enabled (enabled by default).
    d) Enable Kerberos.
    e) Enable Kerberos and pass-through authentication with smart card.
    f) Enable Anonymous access on the IIS Default website and use Integrated Windows Authentication.
    g) Ensure that the IIS Default website doesn't require SSL and ignores client certificates.
2. Use the Group Policy Management Console to configure Local Computer Policies on the user device.
    a) Import the Receiver.admx template from %Program Files%\Citrix\ICA Client\Configuration\.
    b) Expand **Administrative Templates** > **Classic Administrative Templates (ADMX)** > **Citrix Components** > **Citrix Workspace** > **User authentication**.
    c) Enable Smart card authentication.
    d) Enable Local user name and password.
3. Configure the user device before installing Citrix Workspace app Desktop Lock.
    a) Add the URL for the Delivery Controller™ to the Windows Internet Explorer Trusted Sites list.
    b) Add the URL for the first Delivery Group to the Internet Explorer Trusted Sites list. Add the URL in the form desktop://delivery-group-name.
    c) Enable Internet Explorer to use automatic logon for Trusted Sites.

When Citrix Workspace app Desktop Lock is installed on the user device, it enforces a consistent smart card removal policy. For example, if the Windows smart card removal policy is set to Force logoff for the desktop, the user must log off from the user device, regardless of the Windows smart card removal

© 1997–2026 Citrix Systems, Inc. All rights reserved.

policy set on it. Desktop Lock ensures that the user device isn't left in an inconsistent state. This applies only to user devices with the Citrix Workspace app Desktop Lock.

Remove Desktop Lock

Be sure to remove both of the components listed as follows:

1. Sign in with the same local administrator account that was used to install and configure Citrix Workspace app Desktop Lock.
2. From the Windows feature for removing or changing programs:
    - Remove Citrix Workspace app Desktop Lock.
    - Remove Citrix Workspace app for Windows.

Passing Windows shortcut keys to the remote session

Most Windows shortcut keys are passed to the remote session. This section highlights some of the common ones.

Windows

- Win+D - Minimize all windows on the desktop.
- Alt+Tab - Change active window.
- Ctrl+Alt+Delete - via Ctrl+F1 and the Desktop Viewer toolbar.
- Alt+Shift+Tab
- Windows+Tab
- Windows+Shift+Tab
- Windows+All Character keys

Windows 8

- Win+C - Open charms.
- Win+Q - Search charm.
- Win+H - Share charm.
- Win+K - Devices charm.
- Win+I - Settings charm.
- Win+Q - Search apps.
- Win+W - Search settings.
- Win+F - Search files.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Windows 8 apps

- Win+Z - Get to app options.
- Win+. - Snap app to the left.
- Win+Shift+. - Snap app to the right.
- Ctrl+Tab - Cycle through app history.
- Alt+F4 - Close an app.

Desktop

- Win+D - Open desktop.
- Win+, - Peek at desktop.
- Win+B - Back to desktop.

Other

- Win+U - Open Ease of Access Center.
- Ctrl+Esc - Start screen.
- Win+Enter - Open Windows Narrator.
- Win+X - Open the system utility settings menu.
- Win+PrintScrn - Take a screenshot and save to pictures.
- Win+Tab - Open switch list.
- Win+T - Preview open windows in taskbar.

Software Development Kit (SDK) and API

September 7, 2025

Certificate Identity Declaration SDK

The Certificate Identity Declaration (CID) SDK lets developers create a plug-in. The plug-in lets Citrix Workspace app authenticate to the StoreFront server by using the certificate that is installed on the client machine. CID declares the user's smart card identity to a StoreFront server without performing a smart card-based authentication.

For more information, see the Certificate Identity Declaration SDK for Citrix Workspace app for Windows documentation.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Citrix Common Connection Manager SDK

Common Connection Manager (CCM) SDK provides a set of native APIs that enables you to interact and perform basic operations programmatically. This SDK does not require a separate download because it is a part of the Citrix Workspace app for Windows installation package.

> **Note:**
>
> Some of the APIs that are related to launch require the ICA® file to initiate the launch process to virtual apps and desktops sessions.

The CCM SDK capabilities include:

- Session launch
  - Allows launching applications and desktops using the generated ICA file.
- Session disconnect
  - Similar to the disconnect operation using the Connection Center. The disconnect can be for all the sessions or to a specific user.
- Session logoff
  - Similar to the logoff operation using the Connection Center. The logoff can be for all the sessions or to a specific user.
- Session information
  - Provides different methods to get connection-related information of the sessions launched. The session includes desktop session, application session, and reverse seamless application session

For more information about the SDK documentation, see Programmers guide to Citrix CCM SDK.

Citrix Virtual Channel SDK

The Citrix Virtual Channel software development kit (SDK) supports writing server-side applications and client-side drivers for more virtual channels using the ICA protocol. The server-side virtual channel applications are on Citrix Virtual Apps and Desktops™ servers. If you want to write virtual drivers for other client platforms, contact Citrix Technical support.

The Virtual Channel SDK provides:

- The Citrix Virtual Driver Application Programming Interface (VDAPI) is used with the virtual channel functions in the Citrix Server API SDK (WFAPI SDK) to create new virtual channels. The virtual channel support provided by VDAPI makes it easy to write your own virtual channels.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- The Windows Monitoring API, which enhances the visual experience and support for third-party applications integrated with ICA.
- Working source code for virtual channel sample programs to demonstrate programming techniques.
- The Virtual Channel SDK requires the WFAPI SDK to write the server side of the virtual channel.

For more information, see Citrix Virtual Channel SDK for Citrix Workspace app for Windows documentation.

Fast Connect 3 Credential Insertion API

The Fast Connect 3 Credential Insertion API provides an interface that supplies user credentials to the single sign-on (SSON) feature. This feature is available in Citrix Workspace app for Windows Version 4.2 and later. With this API, Citrix partners can provide authentication and SSO products that use StoreFront to log users on to virtual applications or desktops and then disconnect users from those sessions.

For more information, see Fast Connect 3 Credential Insertion API for Citrix Workspace app for Windows documentation.

ICA® Settings Reference

September 7, 2025

The ICA Settings Reference file provides registry settings and ICA file settings lists, allowing administrators to customize the behavior of the Citrix Workspace app. You can also use the ICA Settings Reference to troubleshoot an unexpected Citrix Workspace app behavior.

ICA Settings Reference (PDF download)

© 2025 Cloud Software Group, Inc. All rights reserved. This document is subject to U.S. and international copyright laws and treaties. No part of this document may be reproduced in any form without the written authorization of Cloud Software Group, Inc. This and other products of Cloud Software Group may be covered by registered patents. For details, please refer to the Virtual Patent Marking document located at https://www.cloud.com/legal. Citrix, the Citrix logo, NetScaler, and the NetScaler logo and other marks appearing herein are either registered trademarks or trademarks of Cloud Software Group, Inc. and/or its subsidiaries in the United States and/or other countries. Other marks are the property of their respective owner(s) and are mentioned for identification purposes only. Please refer to Cloud SG's Trademark Guidelines and Third Party Trademark Notices (https://www.cloud.com/legal) for more information.