Citrix Workspace™ app 1912 LTSR for Windows

Contents

About this release

September 7, 2025

What's new in 1912

Cumulative Update 7 (CU7) is the most recent update to the 1912 LTSR.

Microsoft Teams enhancement

The following Microsoft Teams enhancement is supported for CU6 and later releases:

When Desktop Viewer is in full-screen mode, the user can select one from all screens covered by 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 screens to share. When Desktop Viewer changes the window mode (maximized, restore, or minimize), the screen share stops.

The following Microsoft Teams enhancements are supported for CU5 and later releases:

- Screen sharing improvements - Now when you share your screen, only the Desktop Viewer screen is captured in native bitmap format.
- Peers can now see the presenter's mouse pointer in a screen sharing session.
- Improved video rendering.
- Performance and reliability improvements.
- The WebRTC media engine now honors the proxy server configured on the client device.
- 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.
- You can now 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 now disable the audio device module 2 (ADM2) so that the legacy audio device module (ADM) is used for quad-channel microphones. This 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.

- `DirectWShow` is now the default renderer.

  To change the default renderer, do the following:

  - Launch the Registry editor.
  - Navigate to the following key location: `HKEY_CURRENT_USER\SOFTWARE\Citrix\HDXMediaStream`.
  - Update the following value: `"UseDirectShowRendererAsPrimary"=dword:00000000`

    Other possible values:

    - 0: Media Foundation
    - 1: DirectShow (Default)

  - Relaunch the Citrix Workspace app.

> **Note:**
>
> - The enhancements are supported only on Microsoft Windows 10 Desktop operating system endpoints.
> - The enhancements are not supported on Microsoft Windows 7 and 8 operating system endpoints.
> - The enhancement support is determined during Citrix Workspace app package installation. We recommend that you uninstall Citrix Workspace app when you upgrade the operating system from Microsoft Windows version 7 to version 10.

App Protection

> **Disclaimer**
>
> App Protection policies work by filtering access to required functions of the underlying operating system (specific API calls required to capture screens or keyboard presses). This means that App Protection policies can provide protection even against custom and purpose-built hacker tools. However, as operating systems evolve, new ways of capturing screens and logging keys

> can 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. The feature restricts the ability of clients to be compromised by keylogging and screen capturing malware. App Protection prevents exfiltration of confidential information such as user credentials and sensitive information displayed on the screen. The feature prevents users and attackers from taking screenshots and from using keyloggers to glean and exploit sensitive information.

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

App Protection is configured between StoreFront and the Controller using the Controller. For information about configuring App Protection on the Controller, see App Protection documentation. This configuration is then applied to Citrix Workspace app by including the App Protection component using any of the following methods:

- Graphical user interface
- Command-line interface

You can include the App Protection component both during the Citrix Workspace app installation or on-demand installation.

> **Note:**
>
> - This feature is supported only on Microsoft Windows Desktop operating systems such as Windows 10, Windows 8.1, and Windows 7.
> - This feature is not supported over Remote Desktop Protocol (RDP).

For information about configuring App Protection in Citrix Workspace app, see App Protection.

Enhancement to App Protection Previously, when you are trying to take a screenshot of a protected window, the entire screen, including the non-protected apps in the background, are blacked out.

Now, when you are taking a screenshot using a snipping tool, only the protected window is blacked out or hidden. You can take a screenshot of the area outside the protected window except in non-Aero mode where the entire screen is blacked out.

However, if you are using the **PrtScr** key to capture a screenshot, you must exit the Citrix Workspace app.

Additionally, this release addresses issues to improve the App Protection feature.

Installer enhancement

In earlier releases, if an administrator tried to install Citrix Workspace app on a system that has a user-installed instance of the app, the installation was blocked.

With this release, the administrators can now override the user-installed instance of Citrix Workspace app and continue with the installation successfully.

Enhancement to Citrix Workspace Updates

In earlier releases, if Citrix Workspace app is installed by an administrator, a non-administrator could not update it.

With this release, 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.

> **Note:**
>
> The **Check for Updates** option is now available on both the user-installed and the admin-installed instances of Citrix Workspace app.

Support for outbound proxy

Smart Control allows administrators to define granular policies to configure and enforce user environment attributes for virtual apps and desktops using Citrix Gateway. For instance, you might want to prohibit users from mapping drives to their remote desktops. This can be achieved using the Smart Control feature on Citrix Gateway.

However, the scenario changes when Citrix Workspace app and Citrix Gateway belong to separate enterprise accounts. In such scenarios, the client domain cannot apply the Smart Control feature because the gateway does not exist on the client domain. Instead, you can leverage the, Outbound ICA Proxy. Outbound ICA Proxy lets you use the Smart Control feature even when Citrix Workspace app and Citrix Gateway are deployed in different organizations.

Citrix Workspace app supports session launches using the Citrix ADC LAN proxy. Either a single, static proxy can be configured or the proxy server can be selected at runtime using the outbound proxy plug-in.

You can configure outbound proxies using the following methods:

- Static proxy: Proxy server is configured by providing 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.

You can configure the outbound proxy using the Group Policy Object administrative template and the Registry editor.

For more information about outbound proxy, see Outbound ICA Proxy support in the Citrix Gateway documentation.

For more information about configuring outbound proxy in Citrix Workspace app, see Outbound proxy.

Citrix Embedded Browser binaries

This release no longer installs the Citrix Embedded Browser. In cases where you upgrade to Version 1912, the Citrix Embedded Browser is removed.

In the absence of Citrix Embedded Browser, the following functionalities change:

- Browser content redirection does not function.
- SaaS and Web apps are not launched using the Citrix Embedded Browser. Instead they are launched in the Citrix Secure Browser Service.

Enhancement to desktop sharing with Microsoft Teams

When you share your workspace using Microsoft Teams, Citrix Workspace app displays a red border that surrounds 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.

Endpoint encoder performance estimator on Microsoft Teams

When the HdxTeams.exe process (the WebRTC media engine embedded in Citrix Workspace app that handles Microsoft Teams redirection)is launched, it estimates the best encoding resolution that the endpoint's CPU can sustain without overloading. Possible values are 240p, 360p, 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 achieved with the particular endpoint. The highest possible resolution is then included during the codec negotiation between the peers, or between the peer and the conference server.

For information on configuring endpoint encoder, see Endpoint encoder performance estimator on Microsoft Teams.

For information, see Optimization for Microsoft Teams in Citrix Virtual Apps and Desktops documentation.

Enhancement to Citrix Analytics Service

With this release, Citrix Workspace app is instrumented to securely transmit the public IP address of the most recent network hop to Citrix Analytics Service. This data is collected per session launch. It helps Citrix Analytics Service to analyze whether poor performance issues are tied to specific geographic areas. By default, the IP address logs are sent to Citrix Analytics Service. However, you can disable this option on the Citrix Workspace app using the Registry editor.

To disable IP address log transmissions, navigate to the following registry path and set the `SendPublicIPAddress` key to **Off**.

- On 64-bit Windows machines, navigate to : `HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Citrix\Dazzle`.
- On 32-bit Windows machines, navigate to: `HKEY_LOCAL_MACHINE\SOFTWARE \Citrix \Dazzle`.

> **Note:**
>
> - Although Citrix Workspace app transmits every IP address that it is launched on, IP address transmissions are best-case efforts. Some of the addresses might not be accurate.
> - In closed customer environments, where the endpoints are operating within an intranet, ensure that the URL `https://locus.analytics.cloud.com/api/locateip` is whitelisted on the endpoint.

For more information on how Performance Analytics uses this information, see Self-Service for Performance.

Fixed issues

September 7, 2025

Citrix Workspace app 1912 LTSR CU7 for Windows

Compared to: Citrix Workspace app 1912 LTSR CU6

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]

Logon/Authentication

- Attempts to add Citrix Gateway URL might fail intermittently with this error message:

  Authentication Service cannot be contacted.

  [CVADHELP-19415]

Session/Connection

- Using the Storebrowse utility to enumerate resources for the Citrix Gateway URL might fail when at least one of the configured Delivery Controllers is not reachable. [CVADHELP-15416]
- When Citrix IME is enabled, certain third-party applications might not respond and application launches in a user session might fail. The issue occurs because of the faulting CtxIme module. [CVADHELP-18511]
- Attempts to refresh or launch an app might result in the **cannot contact store** error message. This issue happens when the retrieval of shortcut description for specific subscribed apps fails.

  Your apps are not available at this time. Please try again in a few minutes or contact your help desk with this information: cannot contact store.

  [CVADHELP-18736]
- Attempts to launch a user session might fail after using the **selfservice.exe –init –ipoll –exit** command. [CVADHELP-19095]
- 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]

User Experience

- When the Build to lossless graphics policy is enabled in a multi-monitor environment, spanning the screen across a laptop and an external monitor might result in a distorted image. [CVADHELP-19065]

Citrix Workspace app 1912 LTSR CU6 for Windows

Compared to: Citrix Workspace app 1912 LTSR CU5

Client Device Issues

- In a Citrix Workspace app session, starting a YouTube video or a Microsoft Teams call and then disconnecting the headset might make the session unresponsive. [CVADHELP-17629]

Installing, Uninstalling, Upgrading

- When you upgrade Citrix Workspace app for Windows from Version CU4 to Version CU5 without installing self-service, the following prompt might appear:

  Upgrading from Unsupported Version

  Citrix Workspace will automatically uninstall your old version and delete all your settings, which you can restore later. Otherwise you will have to delete everything manually. Click OK to continue.

  [CVADHELP-18790]

Logon/Authentication

- Logon to Citrix Gateway using an incorrect password lets Storebrowse make multiple authentication attempts that might lock out the user account. [CVADHELP-17467]
- Citrix Workspace app authentication might fail after initialization when attempted using a smart card through Citrix Gateway. If you refresh the authentication process after 15 minutes, a 404-error message might appear in the embedded browser within Citrix Workspace. This results in the app being stuck in the authentication loop until you close and reopen the app. [CVADHELP-18305]

Session/Connection

- Opening a published application using folder redirection when the folder redirection share is offline, might fail with the following error message.

  Unable to launch application

  [CVADHELP-16387]
- When attempting to open an application using the shortcut with the **Limit to one instance per user** and **vPrefer** options enabled, a connection failure error might appear on the Citrix Director. [CVADHELP-17372]
- During a conference call, when using Microsoft Teams in HDX™ optimized mode, the video portion of incoming calls might flicker. [CVADHELP-17398]

- Citrix Workspace app might poll external beacons for internal stores. With this fix, external beacons are not polled when the store is used without the gateway. [CVADHELP-18275]
- Shortcuts for published applications through Citrix Workspace app cannot be created without appropriate permissions. As a result, the icons might be downloaded in the user profile at every refresh, increasing the cache size on the endpoints and the CPU consumption in the StoreFront side. [CVADHELP-18609]
- An optimized Microsoft Teams peer-to-peer call made from Citrix Workspace app for Mac to Citrix Workspace app for Windows might disconnect. [CVADHELP-18696]
- Launching sessions from Delivery Groups with an access policy rule specifying the client IP address might fail if the client has multiple NICs.

  ```
  Rule: Set-BrokerAccessPolicyRule -Name <rulename> -includedClientIPs
   <Client ip address>
  ```

  [CVADHELP-18783]

System Exceptions

- Citrix Authentication Manager (AuthManSvr.exe) might exit unexpectedly during logon. [CVADHELP-17233]

User Experience

- When you open a desktop window in windowed mode in a multi-monitor environment, the following behavior might be observed.

  The window opened on monitor 1 and dragged to monitor 2 might appear maximized on monitor 1 instead of on monitor 2.

  [CVADHELP-17373]

User Interface

- With this fix, you can switch to the required account when multiple accounts and the current account registry are configured. [CVADHELP-17718]
- Configuring an enabled and a disabled store together using a Group Policy Object might result in a non X1 or a green bubble user interface instead of an X1 user interface for the first time on the enabled store. [CVADHELP-17942]
- Disabling the store account in Citrix Workspace app might not delete app shortcuts from the **Start** menu or the desktop. [CVADHELP-18260]

Citrix Workspace app 1912 LTSR CU5 for Windows

Compared to: Citrix Workspace app 1912 LTSR CU4

Client Device Issues

- When using Citrix Workspace app 1912 LTSR CU4, the devices connected with COM ports greater than 9 might fail to map within the session. [CVADHELP-17734]

Installing, Uninstalling, Upgrading

- Attempts to upgrade Citrix Workspace App for Windows using the **/forceinstall** parameter might fail. The issue occurs when the Receiver clean-up utility fails to start the cleanup process. [CVADHELP-17656]

Logon/Authentication

- If a Citrix Gateway session times out, Citrix Workspace might not prompt for authentication when launching an application. [CVADHELP-17187]

Seamless Windows

- Some third-party applications might remain in the foreground keeping other launched applications in the background. [CVADHELP-16897]

Security Issues

- Attempts to install Citrix Workspace app 1912 LTSR for Windows might fail when the USB .cat files are signed with a SHA-1 certificate. [CVADHELP-17679]

Session/Connection

- When browsing webpages on some browsers using HTML or animation on a GPU thin client, Citrix Workspace app for Windows might become unresponsive. The issue occurs when the wfica32 process consumes significant amount of memory. [CVADHELP-16172]
- After upgrading Citrix Workspace app for Windows to version 1912 LTSR CU1 or CU2, session reliability might fail. The issue occurs when the Enlightened Data Transport (EDT) protocol is enabled, and the connection is through Citrix Gateway. [CVADHELP-16694]

- Attempts to launch a session through Citrix Workspace app for Windows might fail when the CGP port (2598) is blocked on the endpoint. [CVADHELP-17632]

User Experience

- This fix suppresses the trust account popup by utilizing a new Group Policy Object setting: **Trusted Store Accounts List**. [CVADHELP-16597]
- When using some third-party applications on a VDA, mouse movements might lag. [CVADHELP-16737]

User Interface

- When using Citrix Workspace app 1912 LTSR CU2 for Windows, Start menu shortcuts might not refresh automatically. The issue occurs when a new application is added or a change is made on the back-end. [CVADHELP-17122]
- Setting the **CurrentAccount** value to **AllAccount** under the registry HKEY_LOCAL_MACHINE\Software\Citrix\ might not take effect. The issue occurs when one or more store accounts are present. [CVADHELP-17229]
- When you attempt to log on to Wyse thin client devices using Citrix Workspace app for Windows, the authorization prompt might appear behind the **Desktop Lock** screen. As a result, you cannot log on until you bring the authorization prompt window to the foreground. [CVADHELP-17880]

Citrix Workspace app 1912 LTSR CU4 for Windows

Compared to: Citrix Workspace app 1912 LTSR CU3

Client Device Issues

- With the **Client COM port redirection** policy enabled, attempts to access the Bluetooth device' s COM port might fail. [CVADHELP-14939]

Logon/Authentication

- Attempts to log on to Citrix Workspace app version 1912 LTSR CU3 for Windows might fail when the user name contains umlaut characters. [CVADHELP-17267]

Security Issues

- The Control Flow Guard binary protection might be missing from the binaries. [CVADHELP-16531]

Session/Connection

- When using the screen share feature in Microsoft Teams during a peer to peer call, a black screen might appear. [CVADHELP-15605]
- If the **HDX Adaptive Transport** policy is set to **Preferred** and **EDT MTU Discovery** is enabled, when attempting to launch applications or desktops, a gray or a black screen might appear with a warning message. [CVADHELP-15805]
- The shortcut created for an application might not delete even after you disable the application or change the path of the shortcut. [[CVADHELP-16448]
- Attempts to launch applications through Citrix Workspace app for Windows might fail when connecting or disconnecting a VPN connection through the Citrix Gateway. [CVADHELP-16714]
- When in a double-hop scenario, the endpoint client names might not pass through to a Delivery Controller™ or Director. The issue occurs with VDA Version 2003 and higher. [CVADHELP-16783]
- After upgrading Citrix Workspace app for Windows to version 1912 LTSR CU1 or CU2, session reliability might fail. The issue occurs when the Enlightened Data Transport (EDT) protocol is enabled, and the connection is through Citrix Gateway. [CVADHELP-16694]

User Experience

- When using Citrix Workspace app Version 1912 LTSR CU2 for Windows, a session might display graphic artifacts that obscure on screen content. [CVADHELP-16451]
- After upgrading Citrix Receiver version 4.9.6 for Windows to Citrix Workspace app version 1912 LTSR CU2 or CU3, attempting to launch an application shortcut, the shortcut icons might flash on some desktops. [CVADHELP-16967]

User Interface

- If you select **Log Out** when a session is running, the **Sign Out** prompt appears to confirm with the action. Pressing **Cancel** will cause an error. [CVADHELP-15516]
- When you upgrade Citrix Receiver version 4.9 LTSR CU7 for Windows to Citrix Workspace app version CU2 or CU3 for Windows and attempt to set the default store account, inconsistent behavior

might occur. For example, the default store account always defaults to All Accounts. With this change, setting the primary store account to a different store name remains even after exiting and restarting Citrix Workspace app. [CVADHELP-16903]

Citrix Workspace app 1912 LTSR CU3 for Windows

Compared to: Citrix Workspace app 1912 LTSR CU2

Installing, Uninstalling, Upgrading

- When you attempt to refresh Citrix Workspace app by using its shortcut that is created manually, the shortcut might get deleted and then recreated. [CVADHELP-15397]

Keyboard

- When you use a Japanese keyboard, the Full-width input mode might fail to work with Microsoft Excel launched through Local App Access. The issue occurs with Citrix Workspace app for Windows that has the App Protection feature enabled. [CVADHELP-15410]

Logon/Authentication

- Even after you enable the **keep me signed in** and **don't ask again for 60 days** policies, Microsoft Azure Multi-Factor Authentication might still prompt for authentication.

  > **Note:**
  >
  > We recommend that users exit their stores rather than log off from their stores. If users log off from stores using webview authentication, they might be prompted for authentication again because Internet Explorer cookies are cleared in such scenarios. By default, the fix is enabled (cookies are stored). You can disable the fix by enabling the **Prevent storing persistent cookies** GPO policy under **Citrix Components > Citrix Workspace > User Authentication**. If you disable the fix, the cookies are not stored and are cleared during logoff. If you disable the fix, the cookies are not stored and are cleared during logoff.

  [CVADHELP-14814]

- On Azure Active Directory (AD) joined devices, when Citrix Workspace app attempts to access a store and then passes through endpoint logon credentials, users might not be authorized to log on. Also, there is no option to log on with a different user account. [CVADHELP-14844]

Printing

- When you send a document in raw data format to the print queue, the document might not be printed. The issue occurs when you use the XPS Printer Driver. [CVADHELP-14497]

Session/Connection

- In certain scenarios, Citrix product license usage shown in Citrix Studio does not match license usage shown in the Citrix License Manager. [CVADHELP-14950]
- With the **vPrefer** option enabled, App-V applications might start on a remote server rather than on a local server. [CVADHELP-15356]
- When you launch a published desktop through a native Citrix Workspace app for Windows, the native Citrix Workspace app automatically runs in the foreground within the desktop. The issue occurs when the **Local App Access** feature is enabled. [CVADHELP-15654]
- The Selfservice.exe process might become unresponsive and a **.NET-BroadcastEventWindow.4.0.0.0.1** prompt might appear. The issue occurs when you attempt to log off from a system running Windows 10 Version 1909. [CVADHELP-15700]
- You configure Citrix Workspace app for Windows to connect to all store accounts when establishing a session. If you log off from Citrix Workspace app and log back on, the store account setting changes to one store account rather than defaulting to all accounts. [CVADHELP-15728]
- With the bidirectional content redirection policy enabled, attempts to redirect a URL from a client to a VDA might fail. [CVADHELP-15739]
- In scenarios where proxy servers do not use port 8080, Citrix Workspace app might fail to connect to published applications and desktops. The issue occurs because Citrix Workspace app for Windows might fail to use the proxy port and use the default port 8080 instead. [CVADHELP-15977]
- Citrix Workspace app for Windows might ignore proxy type settings. The issue occurs with non-English versions of the Microsoft Windows operating system. [CVADHELP-16017]
- When the **EnableFactoryReset** registry setting is set to **False**, attempts to uninstall Citrix Workspace app might fail with this error message:

  This feature has been disabled.

  [CVADHELP-16114]
- With Microsoft Teams in optimized mode, when you join a conference call, audio might become distorted. [CVADHELP-16232]

System Exceptions

- With the **EchoCancellation** policy enabled and audio quality set to medium, the wfica32.exe process might exit intermittently, causing sessions to eventually disconnect. [CVADHELP-14568]
- The Receiver.exe process might exit unexpectedly. [CVADHELP-15669]

Citrix Workspace app 1912 LTSR CU2 for Windows

Compared to: Citrix Workspace app 1912 LTSR CU1

Installing, Uninstalling, Upgrading

- Attempts to upgrade Citrix Workspace app for Windows from Version 190*x* to Version 1912 might fail. The issue occurs when an offending file is present somewhere in the executable folder path. [CVADHELP-15277]
- When you attempt to update Citrix Workspace app from Version 1912 to Version 1912 CU1 or 2006, the update feature of Citrix Workspace app might not work on non-English language operating systems. [CVADHELP-15357]

Keyboard

- When you use the Chinese Input Method Editor (IME) Wuxiami, the shift key might remain stuck in the down position. The issue occurs if the generic local time is set to **ON**. [CVADHELP-15243]

Security Issues

- This fix addresses a security issue. For more information, see Knowledge Center article CTX277662. [CVADHELP-15613]

Session/Connection

- With the registry editing tool disabled, registry keys from the previous installation might not be preserved after you perform an upgrade. As a result, attempts to launch a desktop fail. [CVADHELP-15104]

- Citrix Workspace app might display a script error on versions earlier than 1911 and a blank page on versions 1911 and later. The issue occurs with Stores using Internet Explorer WebBrowser Control to display login pages when Microsoft Security Baseline GPO policies are applied. [CVADHELP-15475]
- In a double-hop scenario, attempts to launch an application using the shortcut in the **Start** menu might fail. The issue occurs if you enable the one-instance-per-user application limit. [CVADHELP-15576]
- When you log on to a Store through Citrix Workspace app Version 1912 or later, applications might fail to enumerate. [CVADHELP-15597]

User Experience

- If you connect to the Self-Service Plug-in (SSP) through a VPN, attempts to refresh the SSP might fail. [CVADHELP-14418]
- Attempts to use the **SelfService.exe -init -ipoll -exit** command to close the SelfService.exe process might fail. [CVADHELP-15126]
- When you use an HP Active stylus pen to write on a published application, the write functionality might experience three to four seconds of delay. [CVADHELP-15203]
- Attempts to launch a session might fail after you do a fresh installation of Citrix Workspace app for Windows or upgrade an existing installation to the latest. The session launch is stuck on the **Preparing your desktop** screen. The issue occurs when you configure Desktop Lock by using a Citrix Gateway URL.

  > **Note:**
  >
  > A black screen appears for some time before Desktop Lock appears the first time you configure Citrix Workspace app for Windows by using a Citrix Gateway URL and Desktop Lock. If the black screen remains for a long time, sign out by using **Ctrl+Alt+Delete** for physical machines and **Ctrl+Alt+End** for virtual machines.

  [CVADHELP-15334]
- After you upgrade Citrix Workspace app to Version 1912 CU1 from Version 1912, application enumeration might be slow, taking about 10 minutes to complete. [CVADHELP-15766]

Citrix Workspace app 1912 LTSR CU1 Hotfix 1 for Windows (19.12.1001)

Compared to: Citrix Workspace app 1912 LTSR CU1 for Windows

Security Issues

- This fix addresses a security issue. For more information, see Knowledge Center article CTX277662. [CVADHELP-15613]

Citrix Workspace app 1912 LTSR CU1 for Windows

Compared to: Citrix Workspace app 1912 LTSR

Content redirection

- When you attempt to redirect a long URL, the URL might not be redirected to a VDA and the Redirector.exe process exits unexpectedly with the following exception:

  INVALID_CRUNTIME_PARAMETER

  [CVADHELP-13197]

Installing, Uninstalling, Upgrading

- Attempts to install or upgrade Citrix Workspace app on a VDA that is running Windows 10 might fail. The issue occurs when you perform the following steps:

  1. Install Citrix Workspace app.
  2. Install a VDA.
  3. Upgrade Citrix Workspace app to a later version.

  The issue occurs because the upgrade or installation causes Citrix display adapters to be removed. [CVADHELP-13764]

- Attempts to use the auto-update functionality to automatically update the HDX RealTime Media Engine (RTME) along with Citrix Workspace app might fail. The RTME fails to upgrade to the latest version. [CVADHELP-15047]

Logon/Authentication

- If you add two stores to Citrix Workspace app for Windows using two different accounts, the Sign-in button might not work for the secondary store after you remove the primary store. [CVADHELP-13805]
- When multifactor authentication is enabled and Windows Security dialog is used to login, the Active Directory Federation Services (ADFS) dialog does not appear when authenticating to stores. [CVADHELP-14316]

- When you configure Citrix Gateway to support single sign-on (SSO) through the Citrix Workspace app, SSO might fail. The issue occurs when a user name or password contains special characters such as **%**, **=**, and **&**. [CVADHELP-14564]

SDK

- This fix provides improved support for legacy private key handles. [CVADHELP-14530]

Session/Connection

- With Local App Access and Desktop Lock enabled, when you perform the Switch user function after pressing the Ctrl+Alt+Del key, the local user session might reconnect. But, when the server session attempts to reconnect, the VDA is stuck on a white screen that displays the message connected to desktop. The desktop never appears. [CVADHELP-13046]
- In a multi-monitor environment, attempts to maximize a user session might fail. The issue occurs when you redock your laptop. [CVADHELP-13614]
- In a double-hop scenario, the Citrix HDX Engine might exit unexpectedly when you attempt to launch a session. [CVADHELP-13915]
- With the **vPrefer** option enabled in Citrix Workspace app, attempts to launch an App-V application might fail with the following error message:

  Cannot start

  [CVADHELP-14039]
- After adding published applications to your **Favorites**, you can open only one application. The issue occurs when those published applications use the same executable name, as indicated by **KEYWORDS:prefer=”<`application_name`>**. [CVADHELP-14098]
- The registry values related to the deprecated feature, **HDX MediaStream for Flash** (for example, Flash and Flash2) might not be removed from the registry setting, HKEY_LOCAL_MACHINE\SOFTWARE\WOW6 Client\Engine\Configuration\Advanced\Modules\ICA 3.0\VirtualDriver after you upgrade the Citrix Workspace app. This issue can cause a connection failure. [CVADHELP-14850]

System Exceptions

- The wfica32.exe process might exit unexpectedly when you attempt to reconnect to a session. The issue occurs with Version 1904.1 of Citrix Workspace app for Windows. [CVADHELP-12807]
- With Local App Access enabled, a session might become unresponsive, displaying the following error message:

Citrix HDX Engine is not responding

[CVADHELP-14058]

- If you attempt to install Citrix Workspace app without configuring self-service mode, an exception might occur. The issue occurs when you open the **Shortcuts and Reconnect** menu from the **Advanced Preferences** sheet. The issue occurs with Citrix Workspace app versions 1907 through 2002. [CVADHELP-14940]

TWAIN

- Attempts to perform scans using a TWAIN device might fail. The **Status** column on the **Applications** tab of the Windows Task Manager displays "Not Responding"for the Citrix HDX Engine. [CVADHELP-14782]

User Experience

- In double-hop scenarios where VDAs for multi-session OS are running in the first hop and published applications are running in the second hop, the Refresh Apps option in the Citrix Workspace app account menu might fail to work. [CVADHELP-13230]
- When you add an account using a store URL on Citrix Workspace app for Windows, it might take a long time to complete. The issue occurs when the URL contains a port number. [CVADHELP-14051]
- You can see two Citrix Workspace app icons in the system tray. The issue occurs with Citrix Workspace app Version 1912. [CVADHELP-14577]
- When you use single sign-on in a VDA environment, a splash screen might appear. The issue occurs when you upgrade Citrix Workspace app for Windows to version 1911 or later. [CVADHELP-14590]

User Interface

- An application might attempt to come to the foreground intermittently, displacing the current application. Its icon in the taskbar might flash, informing the user that the application attempts to come to the foreground. [CVADHELP-13071]

Citrix Workspace app 1912 LTSR for Windows

> **Note:**
>
> If you are a customer currently on the Citrix Workspace app 1911 Current Release and looking to move to the LTSR track:
>
> This release contains the following fixes compared to Citrix Workspace app 1911.
>
> If you are a customer currently on Citrix Receiver 4.9 for Windows and looking to remain on the LTSR track:
>
> This release contains all fixes included in Citrix Receiver for Windows 4.9, including its CUs, through 4.12, and all fixes included in Citrix Workspace app 1808 through 1911, plus the following list of fixes included in Citrix Workspace app 2002 (compared to Citrix Workspace app 1911): Version 1912 contains all the fixes between Citrix Receiver for Windows 4.9 LTSR CU9 and Citrix Workspace app Version 1911 plus the following fixes:

HDX MediaStream Windows Media Redirection

- In a multi-monitor environment, when you play an MP4 video using the Windows Media Player in a user session, the video might play correctly on the primary monitor. But, when you move the player to a different screen, a black screen might appear on the secondary or an extended monitor connected through DisplayLink using a docking station. [CVADHELP-11848]

Session/Connection

- When you attempt to reconnect to a session from the HDX RealTime Media Engine using a fast smart card, the HDX RealTime Media Engine might exit unexpectedly. [CVADHELP-12605]
- When published applications receive many requests to play short sounds for a short period of time, the wfica32.exe process might exit unexpectedly. [CVADHELP-12855]
- After a session timeout is reached, the session might automatically log off. When you attempt to launch the session again, the session takes longer than normal to launch. The issue occurs when there is a network disruption. [CVADHELP-13017]
- A seamless application window might be rendered partially truncated and remain truncated until you manually resize the window. [CVADHELP-13108]
- Citrix Workspace app now performs a check of the presence of shortcut icons every time it refreshes or starts. If an icon is not available, Citrix Workspace app fetches the icon again. Doing so ensures that shortcuts appear correctly. [RFWIN-15501]
- When attempting to enable the Bidirectional Content Redirection policy (under **Computer Configuration > Administrative Templates > Classic Administrative Templates (ADM) > Citrix Components > Citrix Workspace > User experience**), you are prompted to type a URL-specific

entry even if you do not enable the URL-specific application or desktop overrides. [RFWIN-15867]

System Exceptions

- The Receiver.exe process might exit unexpectedly while capturing the CDF traces. [CVADHELP-13077]

Known Issues

September 7, 2025

Known issues in Citrix Workspace app 1912 LTSR CU7 for Windows

No new issues have been observed in this release.

Known issues in Citrix Workspace app 1912 LTSR CU6 for Windows

- When you share your screen in Microsoft Teams, as a published app, the red border at the bottom of the shared screen does not appear. [LCMRFWIN-4194]

Known issues in Citrix Workspace app 1912 LTSR CU5 for Windows

- When you connect certain third-party remoting application such as mRemoteNG to an endpoint and dock the application toolbar of the published application to the sides, the system might become unresponsive with 100% CPU usage. [LCMRFWIN-4164]
- When you attempt to stop screen sharing during Microsoft Teams optimized calls, the session might become unresponsive intermittently. [LCMRFWIN-4184]

Known issues in Citrix Workspace app 1912 LTSR CU4 for Windows

- During a session, when you click **Check for Updates** and updates are downloaded successfully, the current session is not listed in the **Download successful** dialog. [RFWIN-23152]

Known issues in Citrix Workspace app 1912 LTSR CU3 for Windows

No new issues have been observed in this release.

Known issues in Citrix Workspace app 1912 LTSR CU2 for Windows

No new issues have been observed in this release.

Known issues in Citrix Workspace app 1912 LTSR CU1 for Windows

- Attempts to use the webcam in a WebEx meeting might cause Citrix Workspace app to become unresponsive. The issue occurs when you set the UDP audio to **Medium**.

  As a workaround, navigate to the following path in the Registry Editor and set the following:

  Path: HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\Citrix\ICA Client\Engine\Configuration\Advance

  Name: EchoCancellation

  Type: REG_SZ

  Value: FALSE

  [DOCFB-3805]

Known issues in Citrix Workspace app 1912 LTSR for Windows

- Attempts to capture a screen using the **Print Screen** key might fail. This issue occurs when you minimize a protected Citrix Workspace app session. [RFWIN-15155]
- When you launch Microsoft Word both in a published session and on your local device and delete the store from **Accounts**, the following error message appears when you launch the app on the local device:

  Do you want to find an application in Citrix Workspace to open this file?

  [RFWIN-15884]
- Attempts to launch a session on an SSL-enabled VDA might fail. [RFWIN-16129]
- In a protected desktop session, attempts to take a screenshot of a non-protected session might fail. [RFWIN-16704]
- You might not be able to remove store details that were added using the Group Policy Object (GPO) administrative template using the graphical user interface. [RFWIN-16754]
- Attempts to change the display in a protected session cause the session to exit. [RFWIN-16784]

Third party notices

September 7, 2025

Citrix Workspace app 1912 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

- 1 GB RAM.
- .NET Framework requirements
    - Self-Service plug-in requires NET 4.6.2. It allows you to subscribe to and launch the apps and desktops from the Citrix Workspace app for Windows user interface or command line. For more information, see Using command-line parameters.
- Latest version of Microsoft Visual C++ Redistributable.

    > **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, Citrix Workspace app installer package does not contain the Microsoft Visual C++ Redistributable individual binaries but includes the Microsoft Visual C++ Redistributable installer. The Citrix Workspace app installer checks whether the Microsoft Visual C++ Redistributable package is present on the system during the installation and installs it if necessary. Citrix Workspace app Version 1912 and later requires Microsoft Visual C++ Redistributable Version 14.24.28127.4 or later.

    > **Note:**
    >
    > Attempts to install Citrix Workspace app with non-administrator privileges on a system without the Microsoft Visual C++ Redistributable package 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 and Citrix DaaS (formerly Citrix Virtual Apps and Desktops service), and Citrix Gateway as listed in the Citrix Product Lifecycle Matrix.

Citrix Workspace app is compatible with the following Windows Operating systems:

> **Note:**
>
> The Citrix Gateway End-Point Analysis Plug-in (EPA) is supported on Citrix Workspace. On the native Citrix Workspace app, it is 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 10 32-bit and 64-bit Enterprise Editions. For more information about the compatible Windows 10 operating system, see Windows 10 Compatibility with Citrix Workspace app for Windows. Windows 10 32-bit and 64-bit Pro Editions (supported from Citrix Workspace app 1912 LTSR CU5 for Windows onwards)
Windows 8.1, 32-bit and 64-bit editions (including Embedded edition)
Windows 7, 32-bit & 64-bit editions (Extended Security Update - ESU)
Windows 7 Embedded Standard (Extended Security Update - ESU)
Windows Thin PC
Windows Server 2016
Windows Server 2012 R2, Standard, and, Datacenter editions
Windows Server 2019
Windows Server 2008 R2
Windows 10 Enterprise LTSC 2019
Windows 10 Enterprise 2016 LTSB 1607

Windows 10 Compatibility with Citrix Workspace app for Windows

> **Note:**
>
> - Installing Citrix software versions that are released earlier to the Semi-Annual Channel ver-

> sion is not recommended. Customers who choose to do so will need to validate that any issue generating a support call isn't already addressed with a newer Citrix software version if available, and might be required to upgrade to a newer Citrix software version.
>
> - Once a Windows 10 version reaches End of Service that version is no longer serviced or supported by Microsoft. Citrix supports running its software only on an operating system that is supported by its manufacturer. For information about Windows 10 End of Service, see Microsoft's Windows Lifecycle Fact Sheet.

Citrix Workspace app Version	Windows 10 Enterprise Edition Version number	Build number
1912 CU7 and later	LTSC 2021	19044
1912 CU6 and later	21H2	19044
1912 CU6 and later	21H2	19044
1912 CU5 and later	21H1	19043.1165
1912 CU2 and later	20H2	19042.685
1912 CU1 and later	2004	19041.329
1911 and later	1909	18363.418
1909 and later	1903	18362.116
1812 and later	1809	17763.107
1808 and later	10 1803	17134.376

Supported browsers

For a list of supported browsers, see Accessing stores through Citrix Receiver for Web sites.

Operating system matrix

Operating system supported on touch-enabled devices
Windows 10
Windows 8
Windows 7

Operating system supported on VDA
Windows 10
Windows 8
Windows 7
Windows 2012 R2
Windows Server 2016
Windows 2008 R2

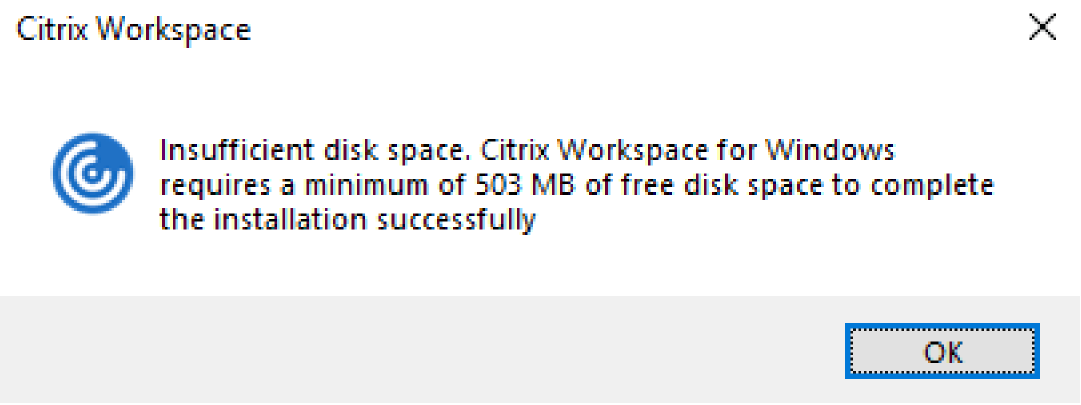
Validating free disk space

The following table provides details on the required disk space to install the Citrix Workspace app for Windows:

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

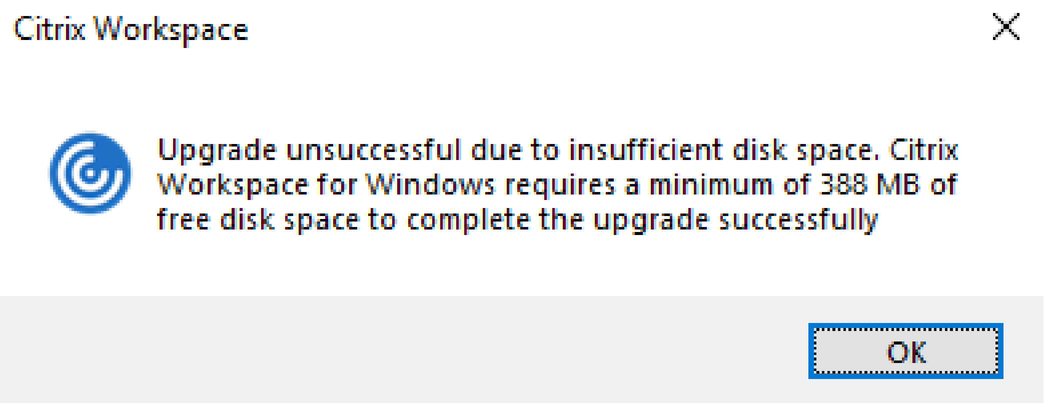
Citrix Workspace app performs a check for the required disk space to complete the installation. The verification is performed both during a fresh installation and an upgrade.

On a fresh install, the installation stops when there is insufficient disk space and the following dialog appears.



Insufficient disk space. Citrix Workspace for Windows requires a minimum of 503 MB of free disk space to complete the installation successfully

During upgrade, the installation ends when there is insufficient disk space and the following dialog appears.



Citrix Workspace

Upgrade unsuccessful due to insufficient disk space. Citrix Workspace for Windows requires a minimum of 388 MB of free disk space to complete the upgrade successfully

> **Note:**
>
> - The installer checks 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`.

Connections, Certificates, and Authentication

Connections

- HTTP store
- HTTPS store
- Citrix Gateway 10.5 and later
- Web Interface 5.4

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 is installed on the remote gateway, the root certificate of the organization's certificate authority must be installed on the user device from which you are accessing the Citrix resources.

> **Note:**
>
> If the remote gateway's certificate cannot be verified upon connection (because the root certificate is not included in the local Keystore.), an untrusted certificate warning appears. If 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 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.

Wildcard certificates

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

Citrix Workspace app supports wildcard certificates; however, they must be used in accordance with your organization's security policy. In practice, an alternative to wildcard certificates is a certificate containing the list of server names with 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 using browsers	StoreFront Services site (native)	StoreFront, Citrix Virtual Apps and Desktops (native), Citrix DaaS	Citrix Gateway to Workspace for Web (browser)	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
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.

Authentication to Web Interface Citrix Workspace app supports the following authentication methods (Web Interface uses the term **Explicit** for domain and security token authentication):

	Web Interface (browsers)	Web Interface Citrix Gateway Site	Citrix Gateway to Web Interface (browser)	Citrix Gateway to Web Interface Citrix Gateway Site
Anonymous	Yes			

	Web Interface (browsers)	Web Interface Citrix Gateway Site	Citrix Gateway to Web Interface (browser)	Citrix Gateway to Web Interface Citrix Gateway Site
Domain	Yes	Yes	Yes*	
Domain pass-through	Yes	Yes		
Security token			Yes*	
Two-factor authentication (domain with security token)			Yes*	
SMS			Yes*	
Smart card	Yes	Yes		
User certificate			Yes (Citrix Gateway plug-in)	

* Available only in deployments that include Citrix Gateway, with or without the associated plug-in installed on the device.

For information about authentication, see:

- Configuring Authentication and Authorization in the Citrix Gateway documentation.
- Configure authentication and delegation in the StoreFront documentation.

Certificate revocation list

When you enable the certificate revocation list (CRL) checking, Citrix Workspace app checks to see if the server's certificate is revoked. Performing this check helps improve the cryptographic authentication of the server and the overall security of the TLS connection between the user device and a server.

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

Exit the Citrix Workspace app and close all the Citrix Workspace components, including the **Connection Center**.

For more information, see the TLS section.

Install and Uninstall

September 7, 2025

Notes to administrators before installing Citrix Workspace app 1912 LTSR for Windows

- Citrix Workspace app 1912 LTSR for Windows requires .NET Framework Version 4.6.2 or later. The Citrix Workspace app installer downloads and installs the .NET Framework, if it is not present on your system. However, we recommend that you install the required .NET Framework manually before installing or updating Citrix Workspace app.
- If you are attempting an unattended install, see Knowledge Center article CTX257546.

You can install the Citrix Workspace app by downloading the `CitrixWorkspaceApp.exe` installation package from the Download page or from your company's download page (if available). You can install the package by:

- 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 the command-line interface, see Using command-line parameters.

Installation with administrator and non-administrator privileges:

Both user and an administrator 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:**
>
> If a user-installed instance of Citrix Workspace app for Windows exists on the system and an administrator installs Citrix Workspace app for Windows on the same system, there will be a conflict. Citrix recommends that you uninstall all user-installed instances of Citrix Workspace app for Win-

> dows before installing Citrix Workspace app for Windows as an administrator.

Using a Windows-based installer

You can install Citrix Workspace app for Windows using the installation media, a network share, Windows Explorer, or a command line by manually running the `CitrixWorkspaceApp.exe` installer package.

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

1. Launch the `CitrixWorkspaceApp.exe` file and click **Start**.
2. Read and accept the End User License Agreement and proceed with the installation.
3. If you are attempting the installation on a domain-joined machine with administrator privileges, an additional dialog appears to enable or disable Single Sign-on. See Domain pass-through authentication for more information.
4. Follow the Windows-based installer to complete the installation.

Using command-line parameters

You can install Citrix Workspace app by typing the installer filename, installation commands, and installation properties from the command line interface. You can customize the Citrix Workspace app installer by specifying command line options. The installer package self-extracts to the system temp folder before launching Setup. The space requirement includes program files, user data, and temp folders after launching several applications.

To install the Citrix Workspace app using the Windows command-line, launch the command prompt and then type the installer filename, installation commands, and installation properties on a single line. The available installation commands and properties are listed below:

```
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 installation commands and properties.
- /`silent` - Disables installation dialogs and prompts during installation.
- /`noreboot` - Suppresses the prompts to reboot dialog during installation. When you suppress the reboot prompt, USB devices that are in a suspended state are not recognized by Citrix Workspace app until after the user device is restarted.
- /`includeSSON` - Requires you to install as an administrator. Indicates that Citrix Workspace app is installed with the single sign-on component. See Domain pass-through authentication for more information.
- /`rcu` - This switch is effective only when upgrading from an unsupported version of the software. Indicates that Citrix Workspace app will be installed or upgraded by uninstalling the existing version. This also cleans up existing 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 on the system in the following scenarios:
  - You are 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.

- Auto (default) - You are notified when an update is available. Example, `CitrixWorkspaceApp.exe /AutoUpdateCheck=auto`.
- Manual - You are not 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 release track you would like to update to. 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`.

`/DeferUpdateCount`

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

- -1(default) - Allows deferring notifications any number of times. Example, `CitrixWorkspaceApp.exe /DeferUpdateCount=-1`.
- 0 - Indicates that you will receive one notification (only) for every available update. You will not be reminded again about the update. Example, `CitrixWorkspaceApp.exe /DeferUpdateCount=0`.
- Any other number 'n'- Allows deferring update 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 released, 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 when using Citrix Virtual Apps and Desktops™ and Citrix DaaS (formerly Citrix Virtual Apps and Desktops service) by restricting the ability of clients to be compromised by keylogging and screen capturing malware.

- `CitrixWorkspaceApp.exe /includeappprotection`

See App Protection for more information.

`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. Example, `CitrixWorkspaceapp.exe ADDLOCAL=ReceiverInside,ICA_Client,AM,SELFSERVICE,DesktopViewer,Flash,Vd3d,WebHelper,BrowserEngine,WorkspaceHub,USB`.

HDX™ features parameters

`ALLOW_BIDIRCONTENTREDIRECTION`

Indicates that the bidirectional content redirection between the client to host and the host to the client is enabled. See the Bidirectional content redirection policy settings section in Citrix Virtual Apps and Desktops documentation for more information.

- 0 (default) –Indicates that bidirectional content redirection is disabled. Example, `CitrixWorkspaceApp.exe ALLOW_BIDIRCONTENTREDIRECTION=0`.
- 1 - Indicates that 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. You must install the Citrix Workspace app with administrator privileges for this component to work. See the Local App Access section in Citrix Virtual Apps and Desktops documentation for more information.

- 0 (default) - Indicates that the local app access component is not installed. Example, `CitrixWorkspaceApp.exe FORCE_LAA=0`.
- 1 - Indicates that the client-side local app access component is installed. Example, `CitrixWorkspaceApp.exe FORCE_LAA=1`.

`LEGACYFTAICONS`

Specifies if application icons are displayed for documents or files that have file type associations with subscribed applications.

- False (default) - Indicates that application icons are displayed 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 does not 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 - Indicates that application icons are not displayed 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.

- 0 (default) - Disables the URL redirection feature on user device. Example, `CitrixWorkspaceApp.exe ALLOW_CLIENTHOSTEDAPPSURL=0`.
- 1- Enables the URL redirection feature on 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 only secure stores (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 stores. Example, `CitrixWorkspaceApp.exe ALLOWADDSTORE=N`.

`ALLOWSAVEPWD`

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

- S(default) - Allows saving the password only for secure stores (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 folder 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`.

`DESKTOPDIR`

Specifies the folder for shortcuts on 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 the **Shortcuts** and **Reconnect** options on the Advanced Preferences sheet. Example, `CitrixWorkspaceApp.exe DisableSetting=0`.
- 1 –Displays only the **Reconnect** option on the Advanced Preferences sheet. Example, `CitrixWorkspaceApp.exe DisableSetting=1`.
- 2 –Displays only the **Shortcuts** option on the Advanced Preferences sheet. Example, `CitrixWorkspaceApp.exe DisableSetting=2`.
- 3 –Both the **Shortcuts** and **Reconnect** options are hidden from the Advanced Preferences sheet. Example, `CitrixWorkspaceApp.exe DisableSetting=3`.

`EnableCEIP`

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

- True (default)- Opt in to CEIP. Example, `CitrixWorkspaceApp.exe EnableCEIP=True`.
- False - Opt out of 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. You must specify a value for the `CLIENT_NAME` property. Example, `CitrixWorkspaceApp.exe ENABLE_DYNAMIC_CLIENT_NAME=No`.

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. This applies only when single sign-on authentication is enabled. For more information, see Domain pass-through authentication with Kerberos.

- Yes - Indicates that the HDX engine will use Kerberos authentication. Example, `CitrixWorkspaceApp.exe ENABLE_KERBEROS=Yes`.
- No - Indicates that the HDX engine will not use Kerberos authentication. Example, `CitrixWorkspaceApp.exe ENABLE_KERBEROS=No`.

In addition to the properties above, 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 - Fully qualified domain name of the server hosting the store.
- IISLocation - Path to the store within IIS. The store URL must match the URL in the StoreFront provisioning file. The store URL is in the following format `/Citrix/store/discovery`. To obtain 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 enables you to deliver disabled stores, giving users the choice of whether or not they access them. When the store status is not specified, the default setting is **On**.
- storedescription - Description of the store, such as `HR App Store`.

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 PNA Services Sites that are using Citrix Gateway.
> - If you configure more than one store, place the Citrix Gateway store URL first in the list. Only one Citrix Gateway store URL configurations are 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 is 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.

Uninstall

Using Windows-based uninstaller:

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

> **Note:**
>
> You get a prompt to uninstall the Citrix HDX RTME package before continuing with the Citrix Workspace app for Windows installation. Click OK to continue the uninstallation.

Using the command line interface:

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

```
CitrixWorkspaceApp.exe /uninstall
```

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

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

> **Note:**
>
> - The registry keys created by receiver.adm/receiver.adml or receiver.admx remain after uninstallation.
> - If you find any entries in the Registry editor after uninstallation, delete them manually.

Deploy

September 7, 2025

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.

- Using Workspace for Web to ensure that the users have installed the Citrix Workspace app for Windows before launching an application from a browser. 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.

Using Active Directory and sample scripts

You can use Active Directory Group Policy scripts to deploy Citrix Workspace app for Windows on systems based on your Active Directory 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 is not present 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 packages and is not authenticated by the script. The shared folder must have Read permission set to EVERYONE.
- **Script Logging Directory**- This specifies the network share where the install logs are copied and is not authenticated by the script. The shared folder must have Read and Write permissions for EVERYONE.
- **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 per-computer and per-user scripts to install and uninstall Citrix Workspace app. The scripts are located on the Citrix Workspace app for Windows Download page.

Deployment type	To deploy	To remove
Per-computer	CheckAndDeployWorkspacePerMachineStartupScript.bat	CheckAndRemoveWorkspacePerMachineSta
Per-user	CheckAndDeployWorkspacePerUserLogonScript.bat	CheckAndRemoveWorkspacePerUserLogonS

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** and copy the appropriate script to the folder displayed.
5. Close the dialog.
6. 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 designated to receive this deployment to the OU 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 designated for the removal to the OU you created.
2. Reboot the user device and log on.
3. Verify that the newly installed package is not listed in the Program and Features.

Using workspace for web

You can deploy Citrix Workspace app for Windows from workspace for web to ensure that you have installed the Citrix Workspace app for Windows before connecting to an application from a browser. Workspace for web site enable you to access StoreFront stores through a web page. If workspace for web site detects that a user does not have a compatible version of Citrix Workspace app for Windows, you are prompted to download and install Citrix Workspace app for Windows.

Email-based account discovery is not supported when Citrix Workspace app for Windows is deployed using workspace for web. If email-based account discovery is configured and a first-time user installs Citrix Workspace app for Windows from Citrix.com, Citrix Workspace app for Windows prompts the user for an email or server address. Entering an email address results in the error message "Your email cannot be used to add an account."

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 Workspace for Web sites 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.

> **Note:**
>
> Only Citrix Receiver for Windows Version 4.5 and later supports SCCM deployment.

There are four parts to completing the deployment of Citrix Workspace app for Windows using SCCM:

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 information about the application such as Name, Manufacturer, Software version, and so on.

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 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 /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** - Enter the version number of the Citrix Workspace app that you are about to deploy.

    > **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 or not 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 click **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**.

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 schedule you configure. Alternatively, 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, 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 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.
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 Device Collections while browsing in Deploy Software wizard.

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

Update

September 7, 2025

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.

Automatic update

Starting with Version 1912 Cumulative Update 4 (CU4), Citrix Workspace Updates log paths are modified. The Workspace Updates logs are present at C:\Program Files(x86)\Citrix\Logs for machine wide update. The logs are present in the user's temp folder for user wide update,

When a new version of the Citrix Workspace app is released, 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 verisons prior to Citrix Workspace app 2104 and Citrix Workspace app 1912 LTSR CU4.
> - If you have configured an SSL intercepting outbound proxy, add an exception to the Workspace auto-update signature service `https://citrixupdates.cloud.com/` and the download location `https://downloadplugins.citrix.com/` to receive updates from Citrix.
> - Your system must have an internet connection to receive updates.
> - By default, Citrix Workspace Updates is disabled on the VDA. This includes RDS multi-user

> server machines, VDI and Remote PC Access machines.
> - Citrix Workspace Updates are disabled on machines where Desktop Lock is installed.
> - Workspace for Web users cannot download the StoreFront policy automatically.
> - Citrix Workspace updates can be limited to LTSR updates only.
> - Citrix HDX RTME for Windows is included in Citrix Workspace Updates. You are notified of the available HDX RTME update on both the LTSR and the current release of the Citrix Workspace app.

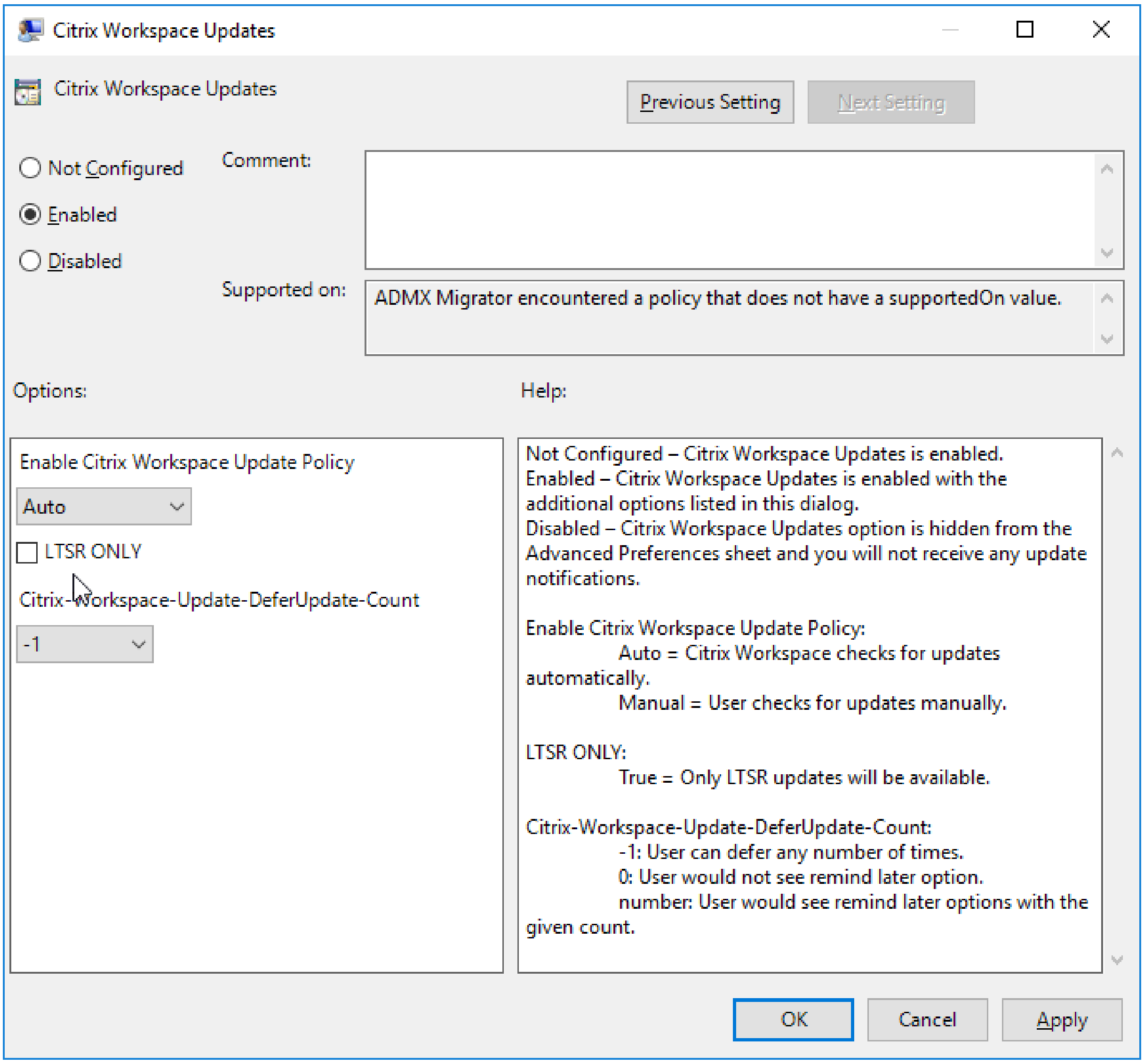
Advanced configuration for automatic updates (Citrix Workspace Updates)

You can configure Citrix Workspace Updates using the following methods:

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

Configure Citrix Workspace Updates using the Group Policy Object administrative template

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



○ Not Configured
● Enabled
○ Disabled

Supported on: ADMX Migrator encountered a policy that does not have a supportedOn value.

Enable Citrix Workspace Update Policy: Auto

□ LTSR ONLY

Citrix-Workspace-Update-DeferUpdate-Count: -1

Not Configured – Citrix Workspace Updates is enabled.
Enabled – Citrix Workspace Updates is enabled with the additional options listed in this dialog.
Disabled – Citrix Workspace Updates option is hidden from the Advanced Preferences sheet and you will not receive any update notifications.

Enable Citrix Workspace Update Policy:
Auto = Citrix Workspace checks for updates automatically.
Manual = User checks for updates manually.

LTSR ONLY:
True = Only LTSR updates will be available.

Citrix-Workspace-Update-DeferUpdate-Count:
-1: User can defer any number of times.
0: User would not see remind later option.
number: User would see remind later options with the given count.

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

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

2. **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 Update Policy** drop-down:

   - Auto - You are notified when an update is available (default).
   - Manual - You are not notified when an update is available. Check for updates manually.

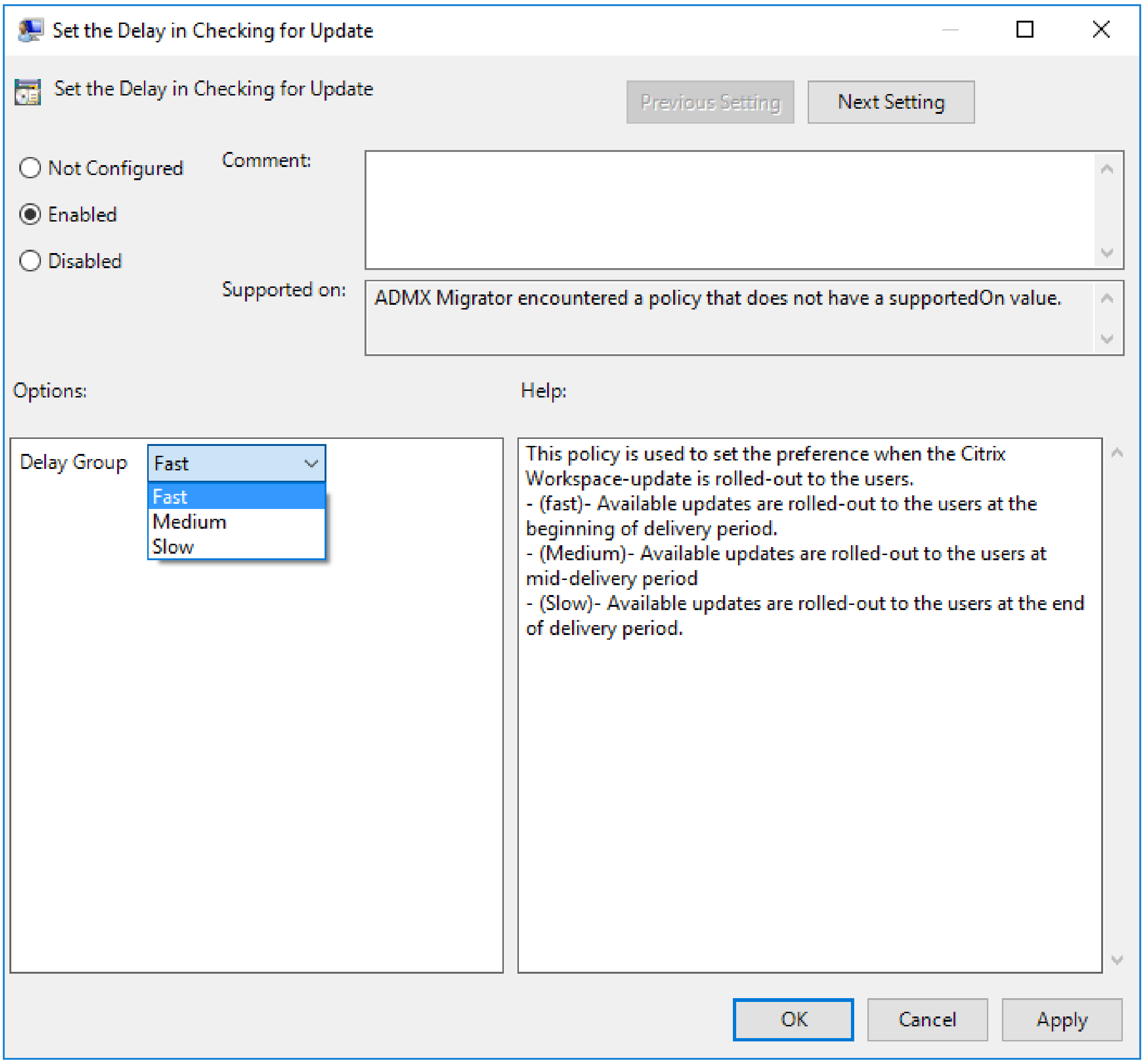
3. Select **LTSR ONLY** to get updates for LTSR only.

4. From the **Citrix-Workspace-Update-DeferUpdate-Count** drop-down, select a value between -1 and 30:

   - -1 - Allows deferring the notifications any number of times (default).
   - 0 - You will receive only one notification for the update.

Configure the delay in checking for updates When a new version of Citrix Workspace app is available, Citrix rolls 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**.



○ Not Configured
● Enabled
○ Disabled

Supported on: ADMX Migrator encountered a policy that does not have a supportedOn value.

Delay Group: Fast
Fast
Medium
Slow

This policy is used to set the preference when the Citrix Workspace-update is rolled-out to the users.
- (fast)- Available updates are rolled-out to the users at the beginning of delivery period.
- (Medium)- Available updates are rolled-out to the users at mid-delivery period
- (Slow)- Available updates are rolled-out to the users at the end of delivery period.

Select **Enabled**, and from the **Delay Group** drop-down, 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 are not notified of the available updates. This also hides the Workspace Updates option from the Advanced Preferences sheet.

Configure Citrix Workspace Updates using the command-line interface

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

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

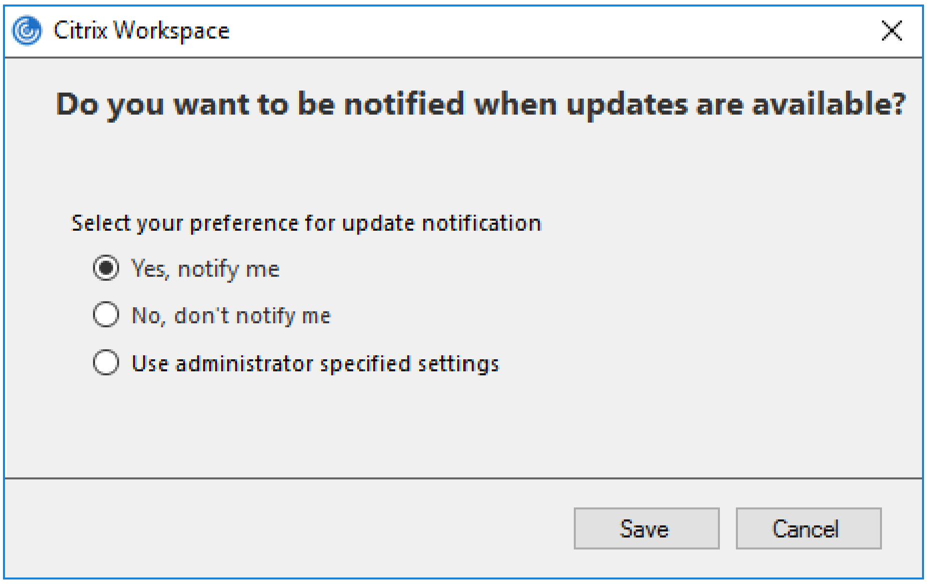
For example,

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

> **Note**:
>
> `/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 over-ride 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. Right-click Citrix Workspace app icon from the notification area. Select **Advanced Preferences** > **Workspace Updates**. Select the notification preference and click **Save**.



Do you want to be notified when updates are available?

Select your preference for update notification

● Yes, notify me

○ No, don't notify me

○ Use administrator specified settings

> **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 the Advanced Preferences sheet section.

Configure Citrix Workspace Updates using StoreFront

1. Use a text editor to open the `web.config` file, which is typically located in the `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 *<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>

            <properties>

              <property name="Auto-Update-Check" value="auto" />

              <property name="Auto-Update-DeferUpdate-Count" value
                 ="1" />

                      <property name="Auto-Update-LTSR-Only" value
                         ="FALSE" />

              <property name="Auto-Update-Rollout-Priority" value=
                 "fast" />

                    </properties>

          </metadata>

        </annotatedServiceRecord>

      </annotatedServices>

      <metadata>

        <plugins>

          <clear />

        </plugins>

        <trustSettings>

          <clear />

        </trustSettings>

        <properties>

          <clear />

        </properties>

      </metadata>

    </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 release update is for LTSR only.
- **Auto-update-Rollout-Priority:** Indicates the delivery period in which you can receive the update.
- **Auto-update-DeferUpdate-Count:** Indicates the number of counts that you can defer the notifications for the release updates.

Get started

September 13, 2025

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

Prerequisites:

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

You must configure the following before starting to use the Citrix Workspace app:

- Group Policy Object administrative template
- StoreFront
- Citrix Gateway Store
- Adding store URL to Citrix Workspace app
- Client drive mapping
- Domain Name Service name resolution

Group Policy Object administrative template

Citrix® recommends using the Group Policy Object administrative template to configure rules for network routing, proxy servers, trusted server configuration, user routing, remote user devices, and 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. This is especially useful for applying Citrix Workspace app settings to a number of different user devices throughout the enterprise. To affect 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.

Starting with Citrix Receiver for Windows Version 4.6, the installation directory includes `CitrixBase.admx` and `CitrixBase.adml`, and, administrative template files (receiver.adm or receiver.admx\receiver.adml -depending on the Operating system) in the installation directory.

> **Note:**
>
> The .adm file is for use with Windows XP Embedded platforms only. The .admx/.adml files are for use with Windows Vista/Windows Server 2008 and all later versions of Windows.

If Citrix Workspace app is installed with the VDA, admx/adml files are found in the Citrix Workspace app installation directory. 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 table below for information on Citrix Workspace app templates files and their respective location.

> **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 is not 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 as explained in the procedure below. While importing the latest files, previous settings are retained.

To add the receiver.adm template file to the local GPO (Windows XP Embedded Operating system only):

Citrix recommends that you use the CitrixBase.admx and CitrixBase.adml files to ensure that the options are correctly organized and displayed within the Group Policy Object Editor.

You can use .adm template files to configure both the Local and/or the domain-based GPO.

1. Open the Citrix Workspace app Group Policy Object administrative template by running gpedit.msc.
2. In the left pane of the Group Policy Editor, select the **Administrative Template**s folder.
3. From the **Action** menu, choose **Add/Remove Templates.**
4. Select **Add** and browse to the template file location `\<Installation Directory>\ICA Client\Configuration\receiver.adm`.
5. Select **Open** to add the template and then Close to return to the Group Policy Editor.

   Citrix Workspace app template file is available in the local GPO directory **Administrative Templates > Classic Administrative Templates (ADM) > Citrix Components > Citrix Workspace**.

After the .adm template files are added to the local GPO, the following message is displayed:

“The following entry in the [strings] section is too long and has been truncated:
Click **OK** to ignore the message.

To add the receiver.admx/adml template files to the local GPO (later versions of Windows Operating System):

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

After installing Citrix Workspace app, copy the template files as given in the table below:

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:**
>
> Citrix Workspace app template files are available on local GPO in **Administrative Templates** > **Citrix Components** > **Citrix Workspace** folder only if you add the CitrixBase.admx/CitrixBase.adml to the `\PolicyDefinitions` folder.

StoreFront

Citrix StoreFront authenticates a connection to Citrix Virtual Apps and Desktops, Citrix DaaS (formerly Citrix Virtual Apps and Desktops service), and VDI-in-a-Box, enumerating, and aggregating available desktops and applications into stores that you can access using Citrix Workspace app.

In addition to the configuration summarized in this section, you must also 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:**
>
> When you select the option to show all stores, you might see the old StoreFront user interface.

To configure StoreFront:

Install and configure StoreFront as described in the StoreFront documentation. Citrix Workspace app requires an HTTPS connection. If the StoreFront server is configured for HTTP, a registry key must be set on the user device as described in Using command-line parameters under the **ALLOWADDSTORE** property description.

> **Note:**

> For administrators who need more control, 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 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/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 store behind Citrix Gateway.

In earlier releases, when you add or remove an account using the **Citrix Gateway URL/StoreFront Account List** policy in the GPO, you must reset the Citrix Receiver for the changes to take effect.

Starting with Version 1808, any changes made to the **Citrix Gateway URL/StoreFront Account List** policy is applied in a session when you restart the Citrix Workspace app. A reset is not required.

> **Note:**
>
> Resetting Citrix Workspace app is not required on a fresh installation of Citrix Workspace app Version 1808 and later. In case of an upgrade to Version 1808 and later, reset the Citrix Workspace app for the changes to take effect.

Limitations:

- Citrix Gateway URL must be listed as first followed by StoreFront URL(s).
- Multiple Citrix Gateway URLs are not supported.
- Citrix Gateway URL configured using this method does not support PNA Services site behind Citrix Gateway.

Manage workspace control reconnect

Workspace control lets applications follow users as they move between devices. This enables, for example, 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. This can also be done for domain-joined client devices using Group Policy.

> **Caution**
>
> Editing the registry incorrectly can cause serious problems that may require you to reinstall your operating system. Citrix cannot guarantee that problems resulting from the incorrect use of 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 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 log on
- 11 = combination of both 3 and 8

Disable workspace control for Citrix Workspace app To disable workspace control, create the following key:

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

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

Name: **WSCReconnectModeUser**

Type: REG_SZ

Value data: 0

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:**
>
> Alternatively, you can set the REG_SZ value WSCReconnectAll to false if you do not 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\ 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

Start menu integration and desktop shortcut only mode 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, who need access to a core set of applications in a consistent way.

As a Citrix Workspace app administrator, use a command-line install flags, GPOs, account services, or registry settings to disable the usual "self-service"Citrix Workspace app interface and replace it with a pre-configured Start menu. The flag is called **SelfServiceMode** and is set to true by default. When the administrator sets the **SelfServiceMode** flag to false, the user no longer has access to the self-service Citrix Workspace app user interface. Instead, they can access subscribed apps from the Start menu and via desktop shortcuts - referred to here as a shortcut-only mode.

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

Working with shortcuts

- Users cannot remove apps. All apps are mandatory when working with the **SelfServiceMode** flag set to false (shortcut-only mode). If the user removes a shortcut icon from the desktop, the icon comes back when the user selects Refresh from the Citrix Workspace app system tray icon.

- Users can configure only one store. The Account and Preferences options are not available. This is to prevent the user from configuring additional stores. The administrator can give a user special privileges to add more than one account using the Group Policy Object template, or 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 system tray icon, where they can add and remove accounts.
- Users cannot remove apps using the **Windows Control** Panel.
- You can add desktop shortcuts via a customizable registry setting. Desktop shortcuts are not added by default. After you make any changes to the registry settings, restart the Citrix Workspace app.
- Shortcuts are created in the Start menu with a category path as the default, UseCategoryAsStartMenuPath.

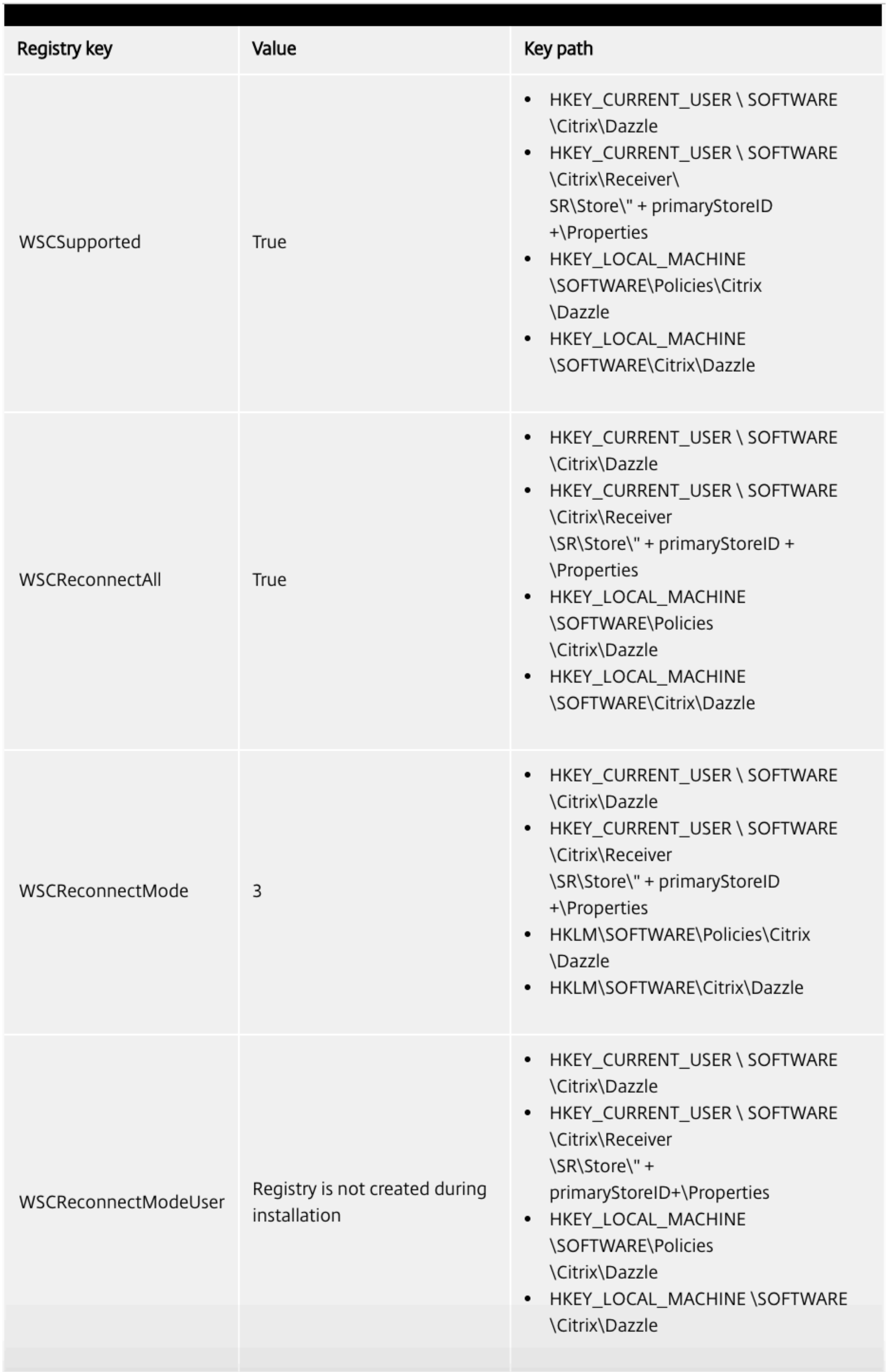
> **Note:**
>
> Windows 8/8.1 and Windows 10 do not allow the creation of nested folders within the Start Menu. Applications are displayed individually or under the root folder but not within Category sub folders defined with Citrix Virtual Apps.

- 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 is a feature which can be enabled via the registry key AutoReInstallModifiedApps. When AutoReInstallModifiedApps are enabled, any changes to attributes of published apps and desktops on the server are reflected on the client machine. When AutoReInstallModifiedApps are disabled, apps and desktop attributes are not updated and shortcuts are not restored on refresh if deleted on the client. By default, this AutoReInstallModifiedApps is enabled. See Using registry keys to customize app shortcut locations.

Customizing location for application shortcut using the Registry editor

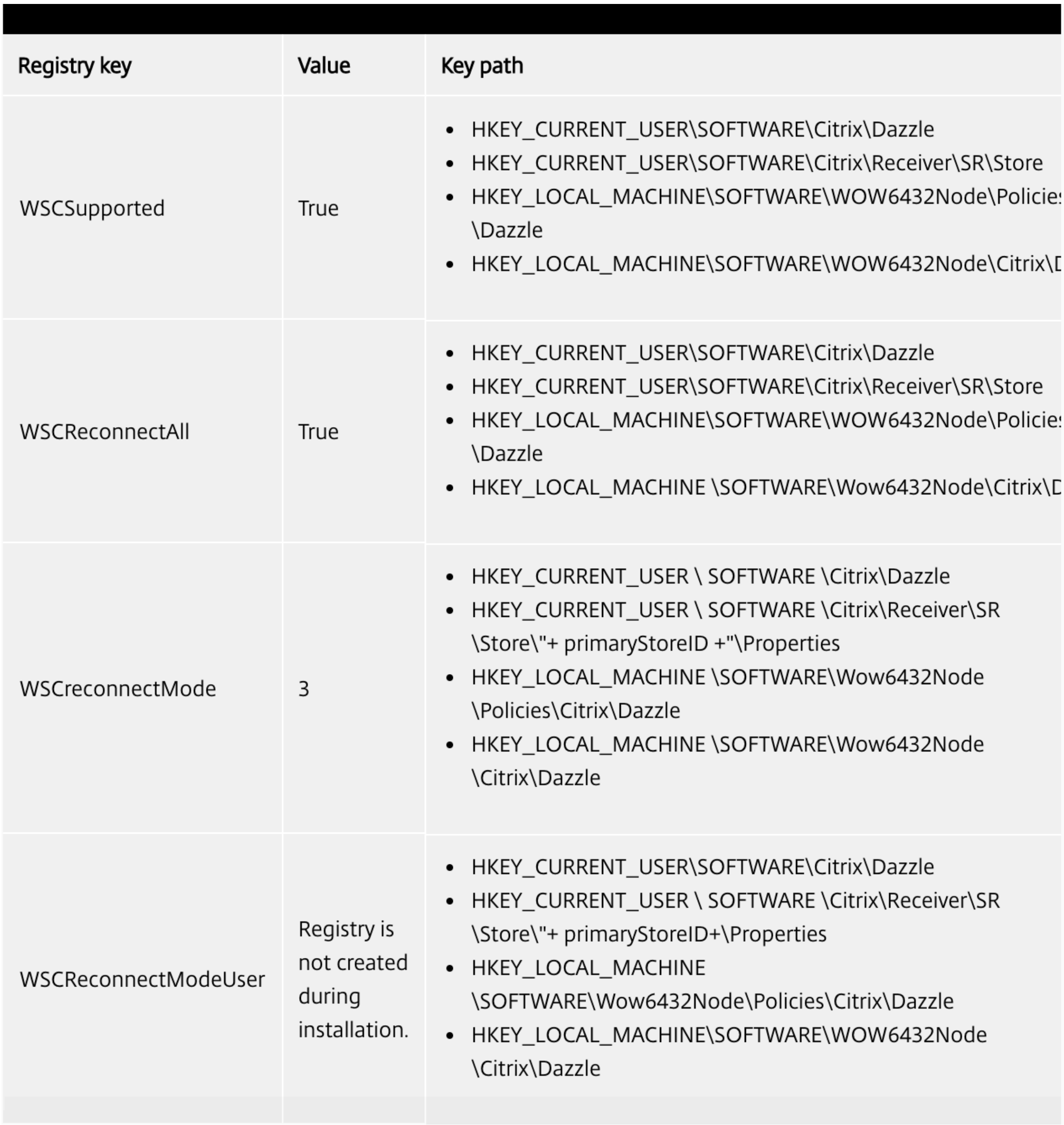
> **Note:**
>
> - By default, registry keys use String format.
> - You should make changes to registry keys before configuring a store. If at any time you or a user wants to customize the registry keys, you or the user must reset Citrix Workspace app, configure the registry keys, and then reconfigure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

Registry keys for 32-bit machines:



Registry key	Value	Key path
WSCSupported	True	• 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
WSCReconnectAll	True	• 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
WSCReconnectMode	3	• HKEY_CURRENT_USER \ SOFTWARE \Citrix\Dazzle • HKEY_CURRENT_USER \ SOFTWARE \Citrix\Receiver \SR\Store\" + primaryStoreID +\Properties • HKLM\SOFTWARE\Policies\Citrix \Dazzle • HKLM\SOFTWARE\Citrix\Dazzle
WSCReconnectModeUser	Registry is not created during installation	• 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	Value	Key path
WSCSupported	True	• HKEY_CURRENT_USER\SOFTWARE\Citrix\Dazzle • HKEY_CURRENT_USER\SOFTWARE\Citrix\Receiver\SR\Store • HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\Policie \Dazzle • HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\Citrix\D
WSCReconnectAll	True	• HKEY_CURRENT_USER\SOFTWARE\Citrix\Dazzle • HKEY_CURRENT_USER\SOFTWARE\Citrix\Receiver\SR\Store • HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\Policie \Dazzle • HKEY_LOCAL_MACHINE \SOFTWARE\Wow6432Node\Citrix\D
WSCreconnectMode	3	• 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
WSCReconnectModeUser	Registry is not created during installation.	• 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. This is to ensure that users can add accounts and Citrix Workspace app can discover USB devices that were in a suspended state during installation.

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.

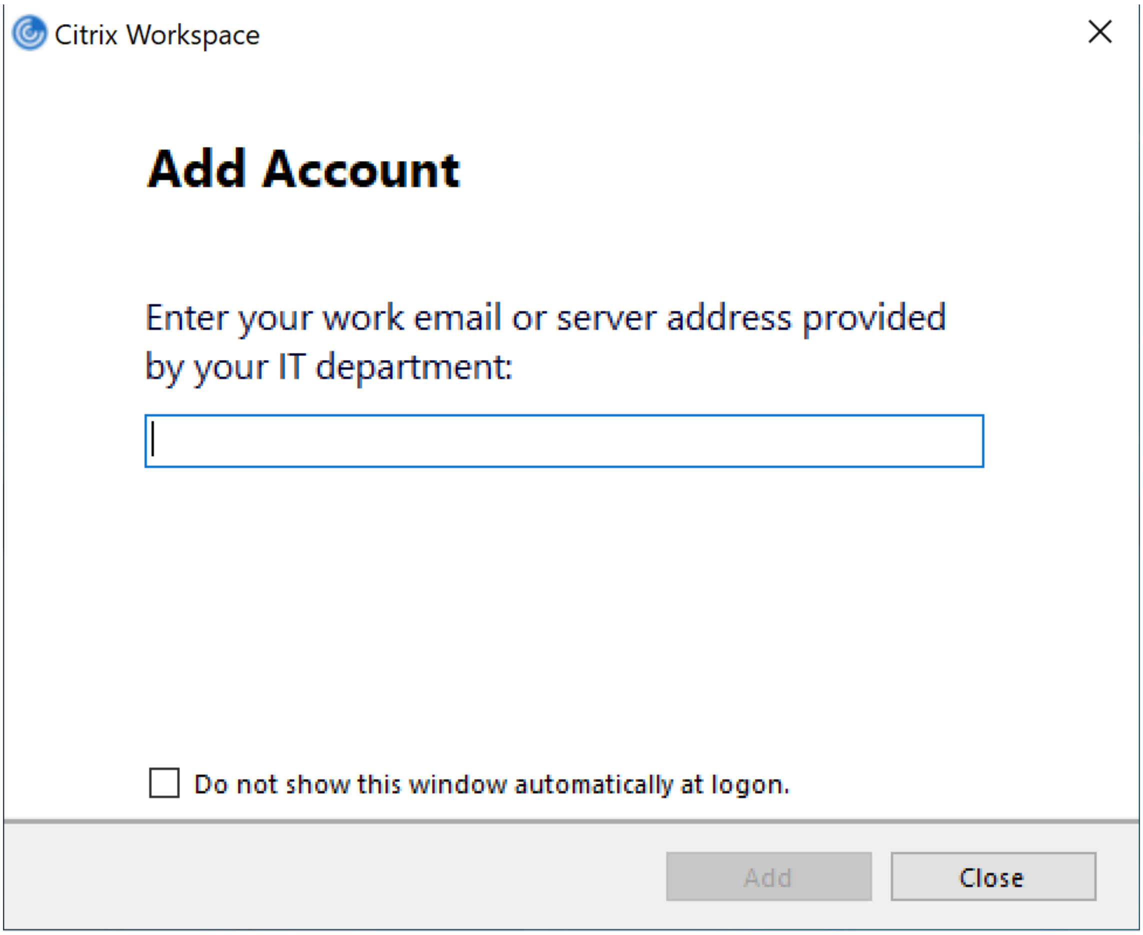
Suppressing Add Account dialog

Add Account dialog is displayed when the store is not configured. Using the **Add Account** dialog, you can set up a Citrix Workspace app account by entering email address or a server URL.

Citrix Workspace app determines the Citrix Gateway, StoreFront server, or App Controller virtual appliance associated with the email address and then prompts the user to log on for enumeration.

Add account dialog can be suppressed in the following ways:

1. **At system logon**



Citrix Workspace

Add Account

Enter your work email or server address provided by your IT department:

□ Do not show this window automatically at logon.

Select **Do not show this window automatically at logon** to prevent the **Add Account** window to pop up on subsequent logon.
This is a per-user setting and resets during Citrix Workspace app for Windows Reset.

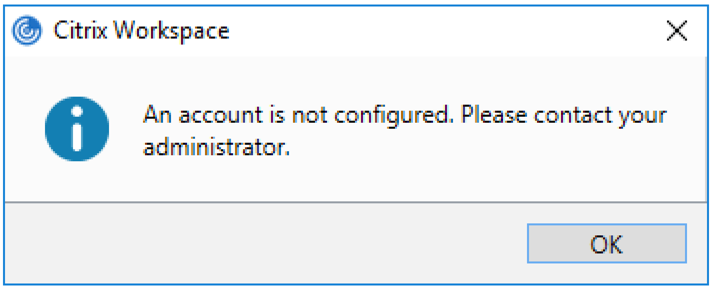
2. **Command line Installation**

   Install Citrix Workspace app for Windows as an administrator using the command line interface with the following switch.

   ```
   CitrixWorkspaceApp.exe /ALLOWADDSTORE=N
   ```

   This is a per-machine setting; hence the behavior shall be applicable for all users.

   The following message is displayed when Store is not configured.

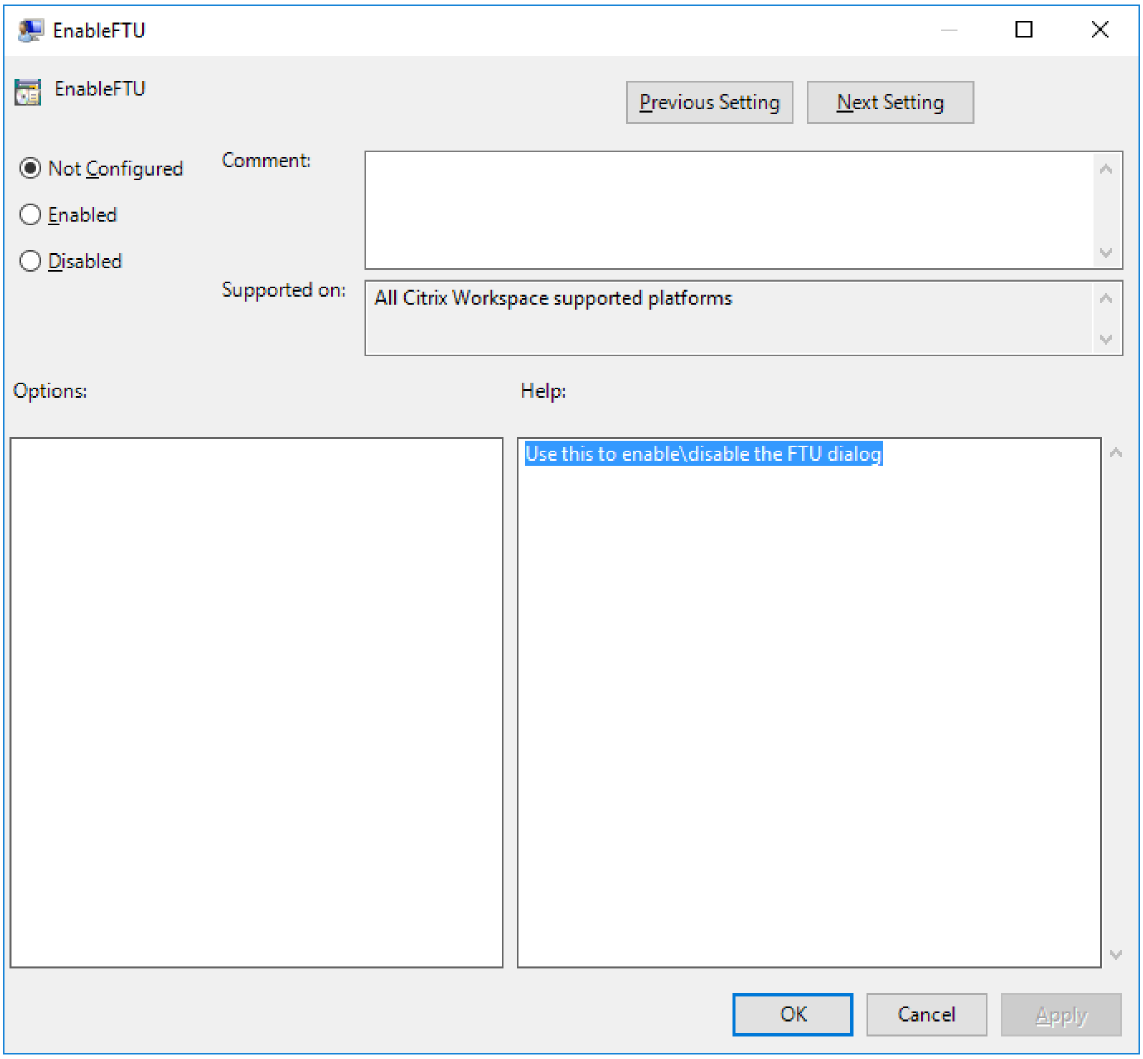


Citrix Workspace

An account is not configured. Please contact your administrator.

Also, **Add Account** dialog can be suppressed in the following ways.

- **Renaming Citrix execution file:**
  Rename the **CitrixWorkspaceApp.exe** to **CitrixWorkspaceAppWeb.exe** to alter the behavior of **Add Account** dialog. When you rename the file, the **Add Account** dialog is not displayed from the Start menu.
- **Group Policy Object administrative template:**
  To hide the **Add Account** option from the Citrix Workspace app installation wizard, disable **EnableFTUpolicy** under Self-Service node in Local Group Policy Object administrative template as shown below.
  This is a per-machine setting, hence the behavior is applicable for all users.



● Not Configured
○ Enabled
○ Disabled

Comment:

Supported on: All Citrix Workspace supported platforms

Help: Use this to enable\disable the FTU dialog

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 and then prompts the user to log on to access virtual desktops and applications.

> **Note:**
>
> Email-based account discovery is not supported for deployments with Web Interface.

For more information about configuring email-based account discovery, see Global App Configuration Service.

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 containing 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 website, users can also obtain 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.

- For connections to a StoreFront store, provide the URL for that server. For example:`https://servername.company.com`.

  For web interface deployments, provide the URL for the Citrix DaaS™ site.

- For connections through Citrix Gateway, first determine whether user should see all configured stores or just the store that has 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 enter server2.com?HRApps to access HRApps. This feature requires that a first-time user create an account by entering a URL and is not available for email-based discovery.

When a user enters the details for a new account, Citrix Workspace app attempts 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**.

Sharing multiple stores accounts automatically

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

If you have 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, create the key "CurrentAccount":

Location: HKEY_LOCAL_MACHINE\Software\Citrix\Dazzle

KeyName: CurrentAccount

Value: AllAccount

Type: REG_SZ

For 64-bit systems, create the key "CurrentAccount":

Location: 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 are 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

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

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.

Turn off 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. When you enable only client drive mapping on the server, client-side full volumes are automatically mapped 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, the portion of the local volume specified by the user is redirected.

Only the user-specified folders appear as UNC links inside 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 allows drive letters on the host-side to be redirected 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:

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

The server can be configured so that the server drive letters do not conflict with the client drive letters; in this case the server drive letters are changed to higher drive letters. For 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	Is accessed 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 a network drive is mapped to the same drive letter as a server drive letter, the network drive mapping is not valid.

When a user device connects to a server, client mappings are reestablished 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, including cameras, scanners, media players, and point of sale (POS) devices to the server. You or the user can restrict 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.

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

A user can set permissions in Citrix Workspace app to always allow or reject device redirection or to be prompted 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 is not 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
   ```

   at a command prompt. The list that appears contains 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.

DNS 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 in the server farm.

Citrix Workspace app connecting to published applications through the Web Interface also use the Citrix XML Service. For Citrix Workspace app connecting through the Web Interface, the Web server resolves the DNS name on behalf of Citrix Workspace app.

DNS name resolution is disabled by default on the server and enabled by default 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 is 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 Registry Editor incorrectly can cause serious problems that can require you to reinstall the operating system. Citrix cannot guarantee that problems resulting from incorrect use of Registry Editor can be solved. Use Registry Editor at your own risk. Ensure you back up 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.

Configure

September 13, 2025

App Protection

> **Disclaimer**
>
> App Protection policies work by filtering access to required functions of the underlying operating system (specific API calls required to capture screens or keyboard presses). This means that App Protection policies can provide protection even against custom and purpose-built hacker tools. However, as operating systems evolve, new ways of capturing screens and logging keys can 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 be compromised by keylogging and screen capturing malware. App Protection prevents exfiltration of confidential information such as user credentials and sensitive information displayed 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 command-line interface or graphical user interface. OR
- During an app launch (on-demand installation).

> **Note:**
>
> - This feature is supported only on Microsoft Windows Desktop operating systems such as Windows 10, Windows 8.1, and Windows 7.
> - This feature is not 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 graphical user interface is available for the purpose.

> **Note:**
>
> Citrix DaaS does not support the App Protection feature.

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

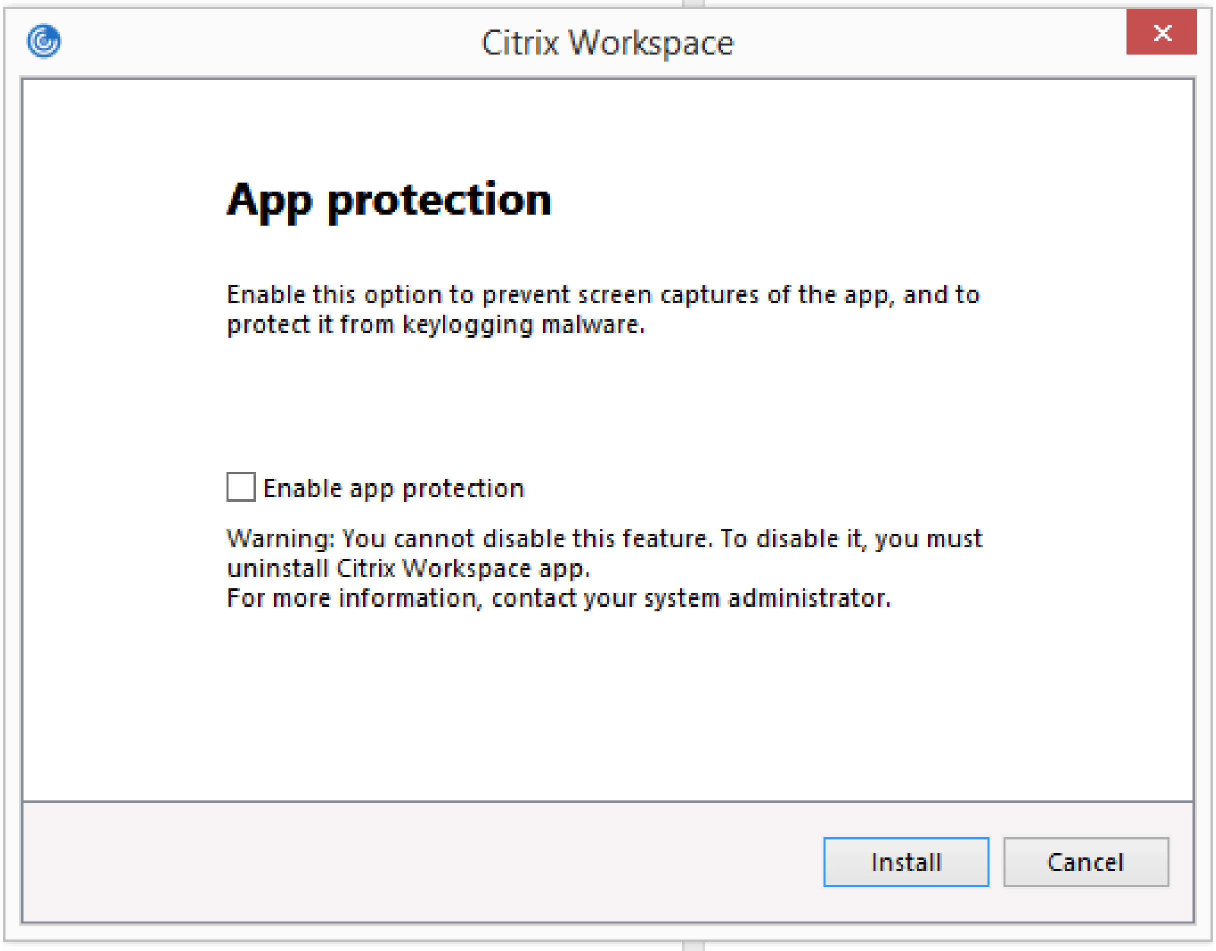
App Protection - Configuration in Citrix Workspace app

> **Note:**
>
> - Include the App Protection component with Citrix Workspace app only if your administrator has instructed you to do so.
> - 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:

- Graphical user interface
- Command-line interface

Graphical user interface 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.



App protection

Enable this option to prevent screen captures of the app, and to protect it from keylogging malware.

□ Enable app protection

Warning: You cannot disable this feature. To disable it, you must uninstall Citrix Workspace app.
For more information, contact your system administrator.

> **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

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

Expected Behavior:

The expected behavior depends upon the method by which users access the StoreFront store containing protected resources.

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

- **Behavior on Workspace for Web:**

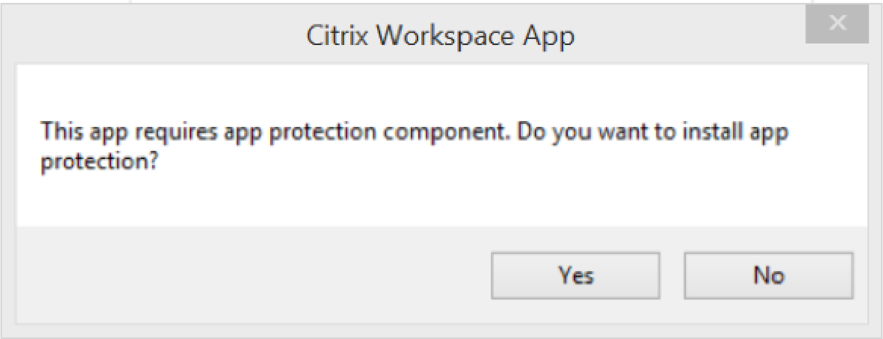
  The App Protection component is not supported on Workspace for Web configurations. Applications protected by App Protection policies are not enumerated. For more information about the resources assigned, contact your system administrator.

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

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

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

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



Citrix Workspace App

This app requires app protection component. Do you want to install app protection?

After clicking **Yes**, App Protection component is installed and the user is able to launch the protected app.

- **Behavior of protected session over Remote Desktop Protocol(RDP)**
    - Your active protected session disconnects if you launch a Remote Desktop Protocol(RDP) session.
    - You cannot launch a protected session in a Remote Desktop Protocol(RDP) session.

App Protection error logs:

The App Protection component 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` –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.

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

Known issues or limitations:

- No feature support on Microsoft Server operating systems such as Windows Server 2012 R2 and Windows Server 2016.
- To take a screen capture of the local device, Citrix Workspace app-related windows must be minimized. Otherwise, you can't perform screen captures of your local device.
- No feature support in double-hop scenarios.
- For this feature to function properly, disable the **Client clipboard redirection** policy on the VDA.

Endpoint encoder performance estimator on Microsoft Teams

When you launch the HdxTeams.exe process (the WebRTC media engine embedded in Citrix Workspace app that handles Microsoft Teams redirection), it estimates the best encoding resolution that the endpoint's CPU can sustain without overloading. Possible values are 240p, 360p, 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 achieved with the particular endpoint. The highest possible resolution is then included during the codec negotiation 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	3
medium	720p	2
slow	360p	1
very slow	240p	0

There are configuration flags to disable the VP9 or H264 codec.
H264 is lighter on the CPU but consumes more bandwidth. On the contrary, VP9 consumes more CPU power but less bandwidth.

Registry Path in Citrix Workspace app:

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

Name	Type	Values	Description
DisableVP9	DWORD	1; 0	1 - disable VP9 codec; 0 - enable
DisableH264	DWORD	1;0	1 - disable H.264 codec; 0 - enable

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 very slow and 3 very fast.

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

Adaptive transport

Adaptive transport is a data transport mechanism for Citrix Virtual Apps and Desktops and Citrix DaaS. It is faster, can scale, improves application interactivity, and is more interactive on challenging long-haul WAN and internet connections. Adaptive transport maintains high server scalability and efficient use of bandwidth. By using adaptive transport, ICA virtual channels automatically respond to changing network conditions. They intelligently switch the underlying protocol between the Citrix protocol called Enlightened Data Transport (EDT) and TCP to deliver the best performance. It improves data throughput for all ICA virtual channels including Thinwire display remoting, file transfer (Client Drive Mapping), printing, and multimedia redirection. The same setting is applicable for both LAN and WAN conditions.

In earlier releases, when **HDXoverUDP** is set to **Preferred**, data transport over EDT is used when possible, with fallback to TCP.

When you enable session reliability, EDT, and TCP attempts to connect in parallel, session reliability reconnection, and auto client reconnect. This enhancement reduces connection time when EDT is preferred but the required underlying UDP transport is unavailable and TCP must be used.

By default, after fallback to TCP, adaptive transport continues to seek EDT every five minutes.

Requirements:

- Citrix Virtual Apps and Desktops 7.12 or later.
- StoreFront 3.8.
- IPv4 VDAs only. IPv6, mixed IPv6 and IPv4 configurations are'nt supported.
- Add firewall rules to allow inbound traffic on UDP ports 1494 and 2598 of the VDA.

> **Note:**

> TCP ports 1494 and 2598 are required and opened automatically when you install the VDA. However, UDP ports 1494 and 2598 are'nt automatically opened. Set them to **Enabled**.

Citrix Workspace app allows the adaptive transport by default. Also by default, the client attempts to use adaptive transport only if the VDA is configured to **Preferred** on the delivery controller and if the setting has been applied on the VDA.

You can enable adaptive transport using the **HDX Adaptive Transport policy** setting. Set the new policy to **Preferred** to use adaptive transport when possible, with fallback to TCP.

Use the Group Policy Object (GPO) administrative template to disable adaptive transport on the client.

To configure adaptive transport using the Citrix Workspace app Group Policy Object (GPO) administrative template

The following are optional configuration steps to customize your environment. For example, you might choose to disable the feature for a particular client for security reasons.

> **Note:**
>
> By default, adaptive transport is disabled (Off) and TCP is always used.

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. Set the **Transport protocol for Citrix Workspace** policy to **Enabled**.
4. Select **Communication Protocol for Citrix Workspace** as required.

   - **Off** - Indicates that TCP is used for data transfer.
   - **Preferred** - Indicates that the client tries to connect to the server using UDP at first. If UDP is unavailable,then the connection switches to TCP as a fallback.
   - **On** - Indicates that the Citrix Workspace app for Windows connects to the server using UDP only. There is no fallback to TCP with this option.

5. Click **Apply** and **OK**.
6. From the command line, run `gpupdate /force` command.

To use adaptive transport, add the Citrix Workspace app template files to the **Policy Definitions** folder. For information on adding template files to the local GPO, see the Group Policy Object template section.

To confirm that the policy setting has taken effect:

Navigate to `HKEY\\_LOCAL\\_MACHINE\SOFTWARE\Policies\Citrix\ICA Client\Engine\Lockdown Profiles\All Regions\Lockdown\Network\UDT` and verify that the **HDXOverUDP** key is included.

For more information, see Adaptive transport section in Citrix Virtual Apps and Desktops documentation.

Advanced Preferences sheet

You can customize the availability and the contents of the **Advanced Preferences** sheet that is present in the right-click menu of the Citrix Workspace app icon in the notification area. Customizing ensures that users can apply only administrator-specified settings on their systems. Specifically, can:

- Hide the Advanced Preferences sheet altogether
- Hide the following, specific settings from the sheet:
  - Data collection
  - Connection Center
  - Configuration checker
  - 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 using the 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 policy for the setting that you want to hide.

The table below lists the options that you can select and the effect of each:

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

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 that of 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.

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 use Workspace for Web or Web Interface site 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*, which allows you to subscribe to applications from the Citrix Workspace app user interface. This 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 - You can configure Citrix Workspace app to automatically place application and desktop shortcuts directly in the Start menu or on the desktop. The new *shortcut only* mode allows you to find the published apps within the familiar Windows navigation schema.

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

Configure self-service mode

Add a StoreFront account to Citrix Workspace app or configure Citrix Workspace app to point to a StoreFront site to use self-serivce mode. Self-service allows users to subscribe to applications from the Citrix Workspace user interface. This enhanced user experience is similar to that of a mobile app store.

> **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 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 **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 **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:

- 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. Applications are displayed individually or under the root folder but not within 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', useDontCreateAddRemoveEntry. 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 may invalidate them. Removing the <clear /> tag when adding a property name and value is optional.

An extended example for this section is:

```
<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 make changes to 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. This functionality was similar to previously released versions of Workspace for Windows, however, release 4.2.100 introduced the ability to control app shortcut placement using Citrix Virtual Apps per app settings. This functionality is useful in environments with a handful of applications that need to be displayed in consistent locations.

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

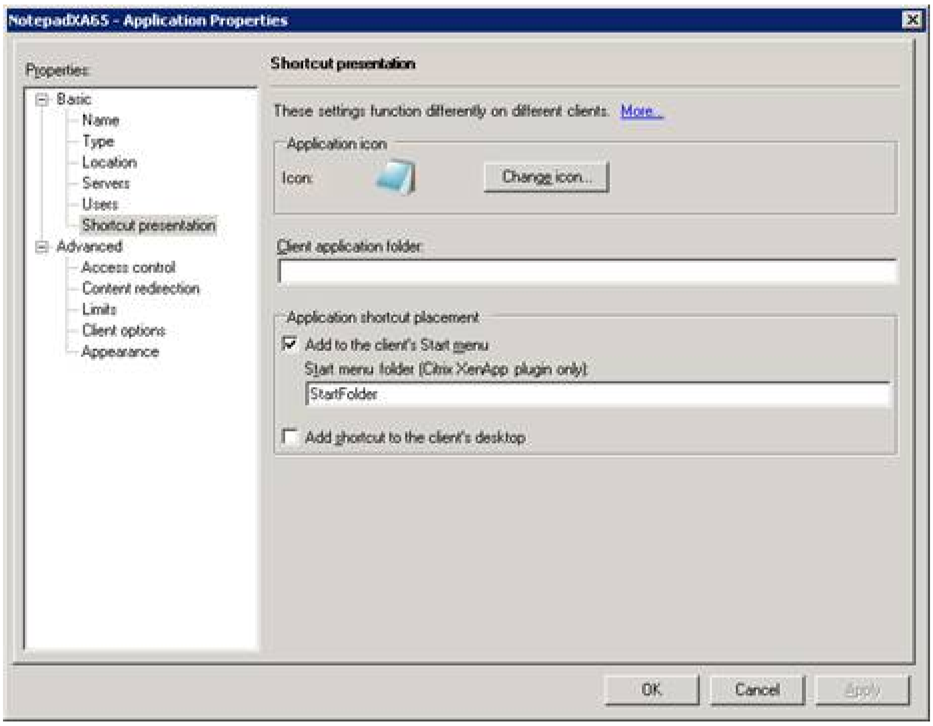
If you want per-app settings to determine where applications are placed independently of whether in self-service mode or Start menu mode.	Configure Citrix Workspace app for Windows with **PutShortcutsInStartMenu**=**false** and enable per app settings. Note: This setting applies to the Web interface site only.

> **Note:**
>
> The **PutShortcutsInStartMenu=false** setting applies to both XenApp 6.5 and XenDesktop 7.x.

Configure per app settings in XenApp 6.5

To configure a per app publishing shortcut in XenApp 6.5:

1. In the **XenApp® Application Properties** screen, expand **Basic** properties.
2. Select the Shortcut presentation option.
3. In the Application shortcut placement portion of the **Shortcut presentation** screen, select the **Add** to the client's Start menu check box. After selecting the check box, enter the name of the folder where you want to place the shortcut. If you do not specify a folder name, XenApp places the shortcut in the Start menu without placing it in a folder.
4. Select the Add shortcut to the client's desktop to include the shortcut on a client machine's desktop.
5. Click **Apply**.
6. Click **OK**.



Shortcut presentation

These settings function differently on different clients. More...

Application icon

Icon:

Client application folder:

Application shortcut placement

☑ Add to the client's Start menu

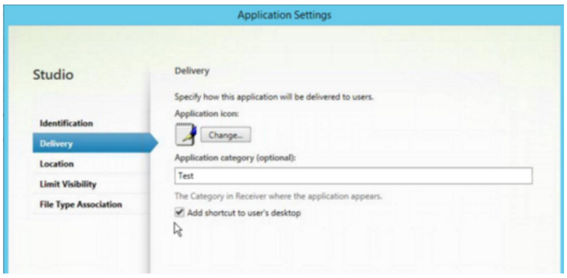
Start menu folder (Citrix XenApp plugin only): StartFolder

☐ Add shortcut to the client's desktop

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 desired 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 check box.
6. Click OK.



Delivery

Specify how this application will be delivered to users.

Application icon:

Application category (optional): Test

The Category in Receiver where the application appears.

☑ Add shortcut to user's desktop

Reducing enumeration delays or digitally signing application stubs

If users experience delays in app enumeration at each logon, or if there is a need to digitally sign application stubs, Citrix Workspace app provides functionality to copy the .EXE stubs from a network share.

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 a white 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 may require you to reinstall your operating system. Citrix cannot guarantee that problems resulting from the incorrect use of Registry Editor can be solved. Use Registry Editor at your own risk. Be sure to backup 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 of the apps. To accomplish this, add all the applications to the machine using Citrix Workspace app. Citrix Workspace app generates the executables.
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 to test the settings.

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, it’s best to allow users to select which applications they want to Favorite and add to the Start menu:

If you want the user to choose the applications 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, 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 and Web interface. You can also configure Citrix Workspace app for self-service access without putting shortcuts anywhere.

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 will not put apps in the Start menu even in self-service mode unless you put them there using per app settings.

All app shortcuts in the Start menu or on the Desktop

If the user has only a few apps, you can put them all in the Start menu or all 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 desktop..	configure Citrix Workspace app with PutShortcutsOnDesktop = true. All available apps appear in 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.

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 if another user is going to share the end point, you can ensure that apps are removed 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 installing 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 application 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 prefer 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 should 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 installing 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.

Starting with 1912, you can configure the automatic refresh behaviour in Citrix Workspace app using the Registry editor.

With earlier releases, when you restart Citrix Workspace app, an automatic refresh occurred even when the cache data is available.

> **Note:**
>
> You cannot configure this option on non-X1 Store accounts.

To configure the automatic refresh using the registry editor:

1. Launch the registry editor and navigate to HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Citrix\Dazzle path.
2. Create the following String Value keys:

Registry key	Value
InitialRefreshMinMs	10000 (10 Second)
InitialRefreshMaxMs	15000 (15 Second)
SuppressRefreshMs	1000 (1 second)

3. Save and close the editor.

> **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 prefer 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.

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

KEYWORDS:prefer=	Shortcut under Programs	Matches?
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.

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.

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

KEYWORDS:prefer=	Shortcut under Programs	Matches?
\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.

Application launch time

Use the session pre-launch feature to reduce application launch time during normal or high traffic periods, thus providing users with a better experience. The pre-launch feature allows a pre-launch session to be created when a user logs on to Citrix Workspace app, or at a scheduled time if the user is already logged on.

This pre-launch session reduces the launch time of the first application. When a user adds a new account connection to Citrix Workspace app for Windows, session pre-launch does not take effect until the next session. The default application ctxprelaunch.exe is running in the session, but it is not visible to you.

Session pre-launch is supported On StoreFront deployments. For Web Interface deployments, be sure to use the Web Interface **Save Password** option to avoid logon prompts. Session pre-launch is not supported for Citrix Virtual Apps and Desktops deployments.

For more information, see Session prelaunch and session linger in a delivery group in Citrix Virtual Apps and Desktops documentation.

Session pre-launch is disabled by default. To enable session pre-launch, specify the `ENABLEPRELAUNCH =`**`true`** parameter on the Workspace command line or set the `EnablePreLaunch` registry key to true. The default setting, null, means that pre-launch is disabled.

> **Note:**
>
> If the client machine has been configured to support Domain Passthrough (SSON) authentication, pre-launch 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 pre-launch:

- **Just-in-time pre-launch**- Pre-Launch 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 pre-launch by restarting the Citrix Workspace app.
- **Scheduled pre-launch**- Pre-launch starts at a scheduled time. Scheduled pre-launch starts only when the user device is already running and authenticated. If those two conditions are not met when the scheduled pre-launch time arrives, a session does not launch. To spread network and server load, the session launches within a window of when it is scheduled. For example, if the scheduled pre-launch is scheduled for 1:45 p.m., the session actually launches between 1:15 p.m. and 1:45 p.m. Typically used for high-traffic periods.

Configuring pre-launch on a Citrix Virtual Apps server consists of creating, modifying, or deleting pre-launch applications, and updating user policy settings that control the pre-launch application.

You cannot customize the pre-launch feature using the receiver.admx file. However, you can change the pre-launch configuration by modifying registry values 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 accomplish this.

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**

Values:

0 - Use the HKEY_LOCAL_MACHINE values even if HKEY_CURRENT_USER values are also present.

1 - Use HKEY_CURRENT_USER values if they exist; otherwise, use the HKEY_LOCAL_MACHINE values.

Name: **State**

Values:

0 - Disable pre-launch.

1 - Enable just-in-time pre-launch. (Pre-Launch starts after the user's credentials are authenticated.)

2 - Enable scheduled pre-launch. (Pre-launch starts at the time configured for Schedule.)

Name: **Schedule**

Value:

The time (24-hour format) and days of week for scheduled pre-launch entered in the following format:

`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 day of the week. For example, to enable scheduled pre-launch on Monday, Wednesday, and Friday at 1:45 p.m., set Schedule as Schedule=13:45	1:0:1:0:1:0:0. The session launches between 1:15 p.m. and 1:45 p.m.

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.

Though Citrix also offers host to client redirection and Local App Access for client to URL redirection, 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:

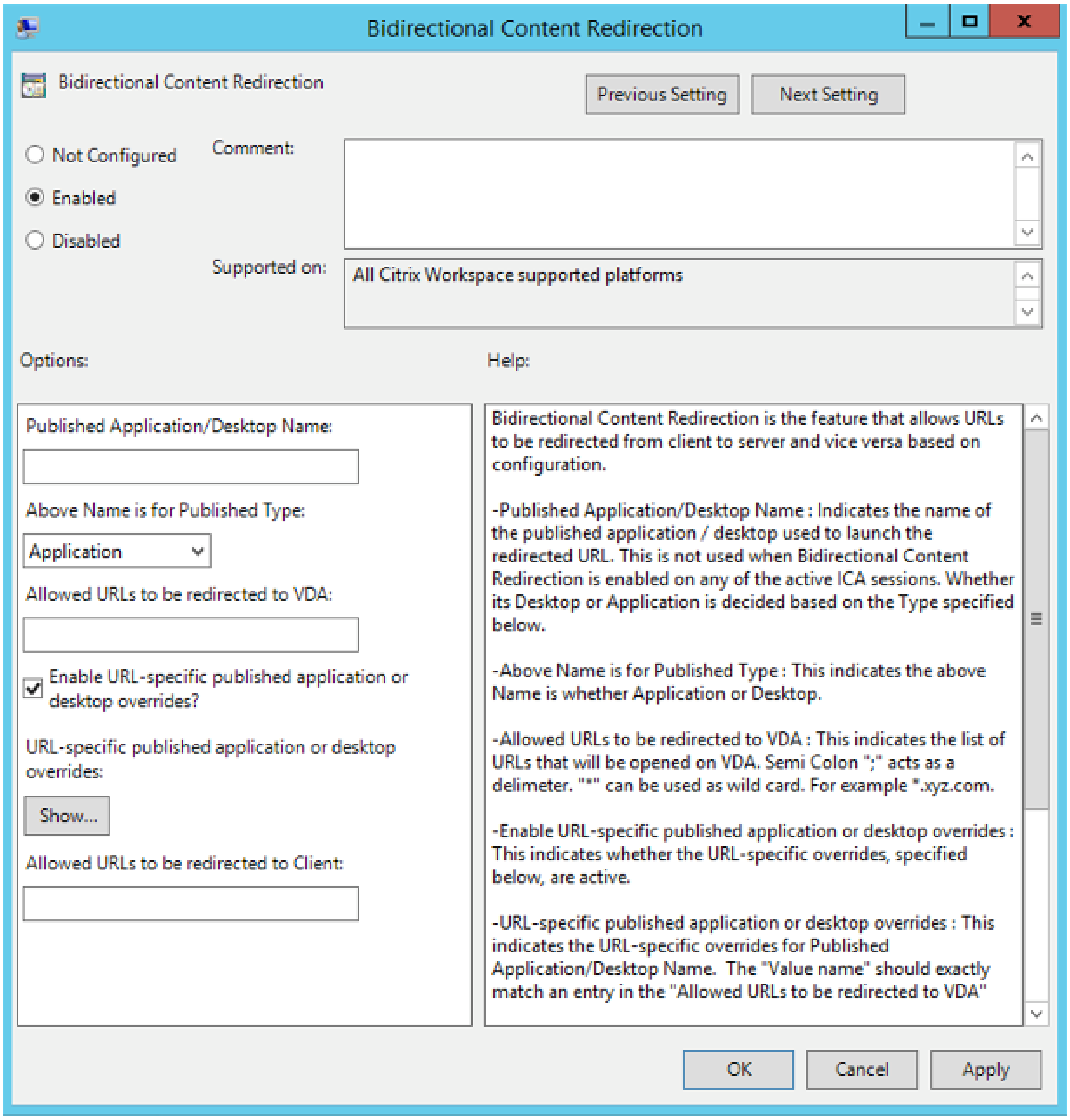
1. Group Policy Object (GPO) administrative template
2. Registry editor

> **Note:**
>
> - Bidirectional content redirection does not work on 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.

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.



Supported on: All Citrix Workspace supported platforms

Published Application/Desktop Name:

Above Name is for Published Type: Application

Allowed URLs to be redirected to VDA:

☑ Enable URL-specific published application or desktop overrides?

URL-specific published application or desktop overrides: Show...

Allowed URLs to be redirected to Client:

Bidirectional Content Redirection is the feature that allows URLs to be redirected from client to server and vice versa based on configuration.

-Published Application/Desktop Name : Indicates the name of the published application / desktop used to launch the redirected URL. This is not used when Bidirectional Content Redirection is enabled on any of the active ICA sessions. Whether its Desktop or Application is decided based on the Type specified below.

-Above Name is for Published Type : This indicates the above Name is whether Application or Desktop.

-Allowed URLs to be redirected to VDA : This indicates the list of URLs that will be opened on VDA. Semi Colon ";" acts as a delimeter. "*" can be used as wild card. For example *.xyz.com.

-Enable URL-specific published application or desktop overrides : This indicates whether the URL-specific overrides, specified below, are active.

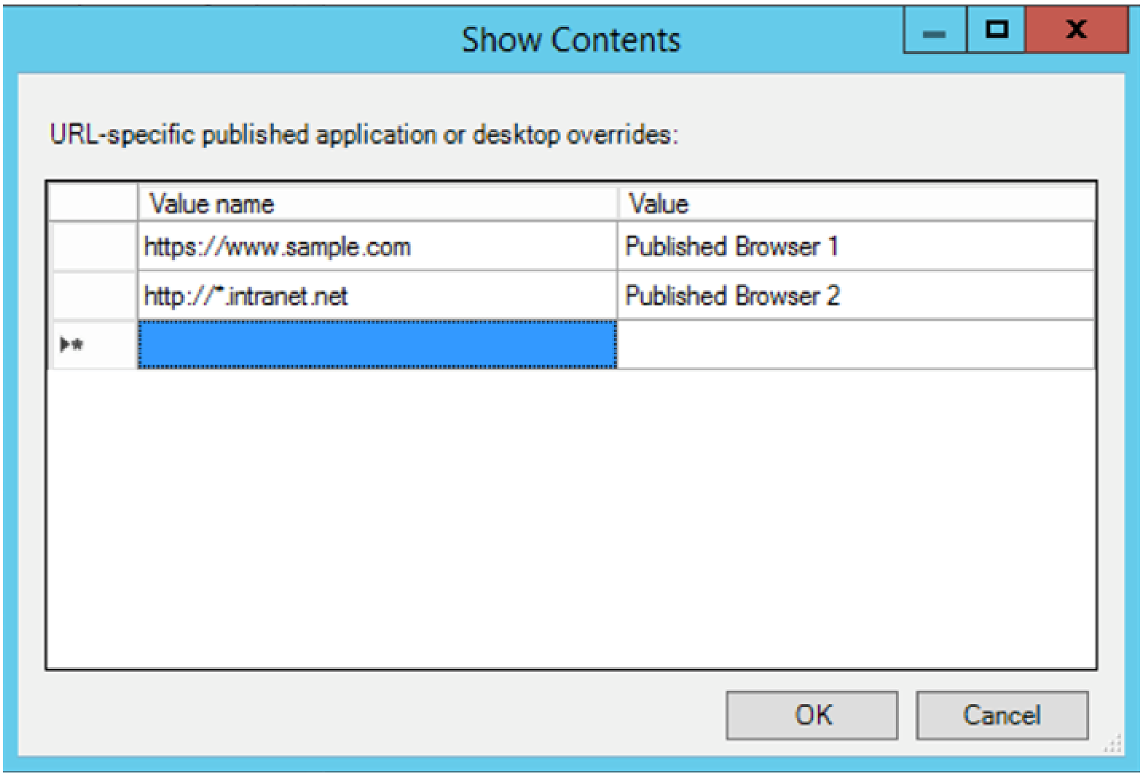
-URL-specific published application or desktop overrides : This indicates the URL-specific overrides for Published Application/Desktop Name. The "Value name" should exactly match an entry in the "Allowed URLs to be redirected to VDA"

1. In the **Published Application/Desktop name** field, provide the name of the resource used to

launch the redirected URL.

> **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 **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.



URL-specific published application or desktop overrides:

	Value name	Value
	https://www.sample.com	Published Browser 1
	http://*.intranet.net	Published Browser 2
▶*		

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.

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 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 (those appearing in the address bar of the browser or found using the in-browser navigation, depending on the browser).
> - If two applications with same display name are configured to use multiple StoreFront accounts, the display name in the primary StoreFront account is used for launching the application or a desktop session.
> - New browser window opens only when URL is redirected to the client. When 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 is supported.
> - Ensure that only one of the server file type association and the host content redirection policies is set to Enabled on the same machine. Citrix recommends that you disable either the server file type association feature or the Host Content (URL) Redirection feature to ensure that URL redirection works properly.

Limitation:

No fallback mechanism is present if the redirection fails due to session launch issues.

Bloomberg keyboards

Citrix Workspace app supports the use of Bloomberg keyboard in a 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.

Multiple sessions with Bloomberg keyboards are not recommended. The keyboard operates in a single-session environment only.

Configure Bloomberg keyboard:

> **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 Registry editor can be solved. Use Registry editor at your own risk. Be sure to back up the registry before you edit it.

1. Locate the following key 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.

For more information on configuring Bloomberg Keyboard, see Knowledge Center article CTX122615.

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, this can make the information on them 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 Registry Editor can be solved. Use 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`
  - `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 that is located 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 is a feature that has the capability to allow you to instantly and securely access 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:

- 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 must not be blocked 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 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

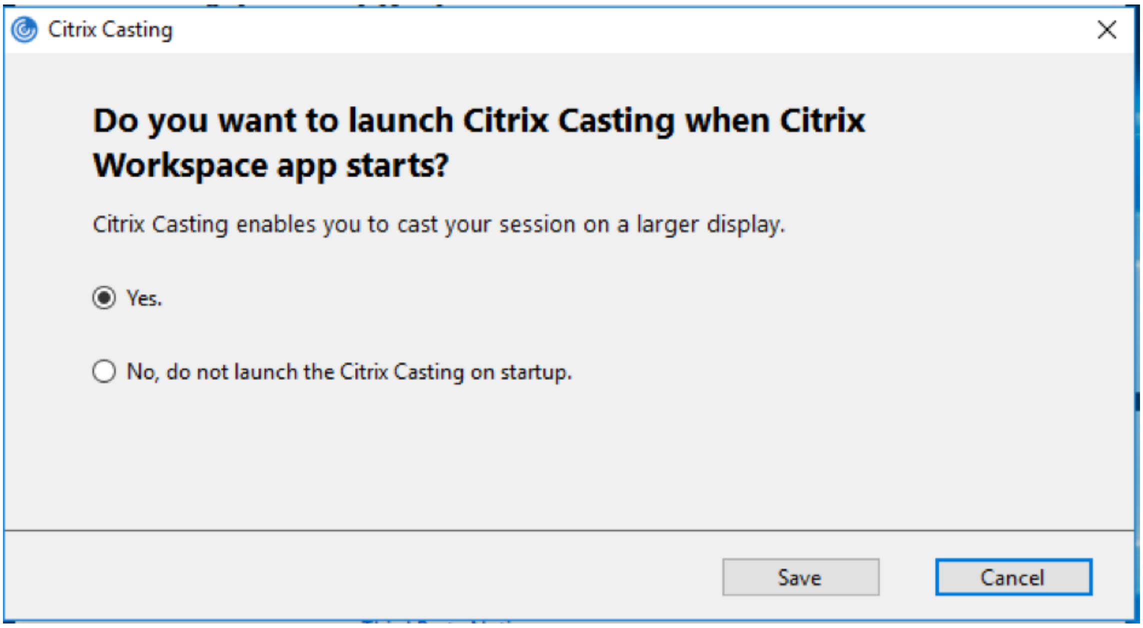
> **Note:**
>
> You can hide all or part of the Advanced Preferences sheet available from the Citrix Workspace app icon in the notification area. For more information, see Advanced Preferences sheet.

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.

   Citrix Casting

   Do you want to launch Citrix Casting when Citrix Workspace app starts?

   Citrix Casting enables you to cast your session on a larger display.

   ● Yes.

   ○ No, do not launch the Citrix Casting on startup.

3. Select one of the options:

   - 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.

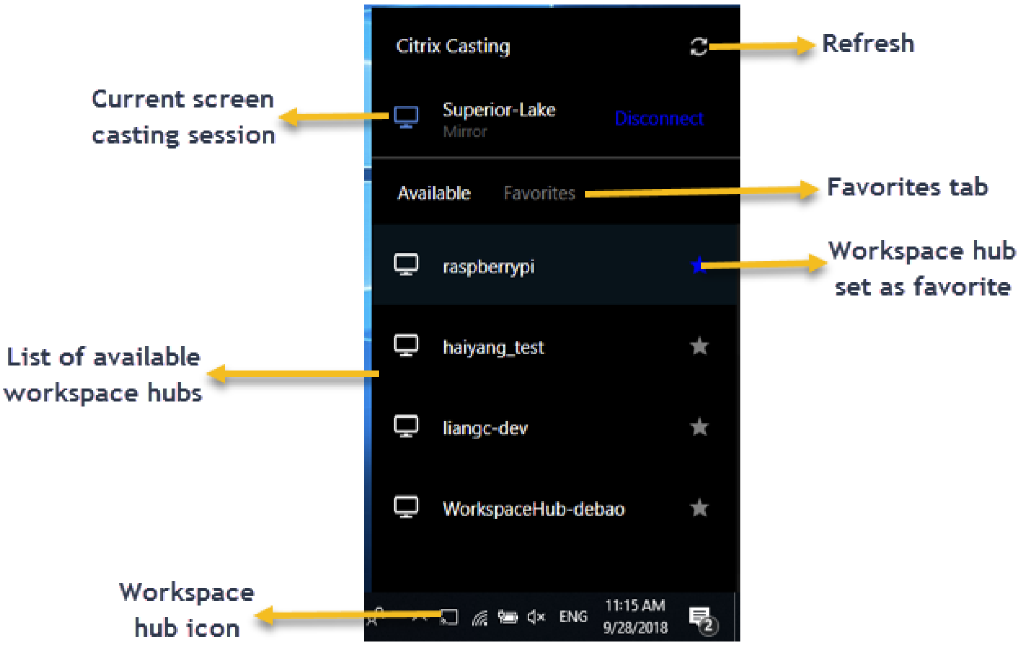
2. Select the workspace hub to cast your screen and choose one of the following:

   - **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.



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 Citrix Ready workspace hub.
4. Launch a browser in Citrix Workspace app and type `http://<hub_ip>:55555/device-details.xml` to check whether the workspace hub device details are displayed.
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. In case of network issues, there might be a lag in display on the workspace hub device.
3. When you select **Extend**, the primary screen where Citrix Ready workspace app is launched flashes multiple times.
4. In **Extend** mode, you cannot set the secondary display as the primary display.

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.

Composite USB device redirection

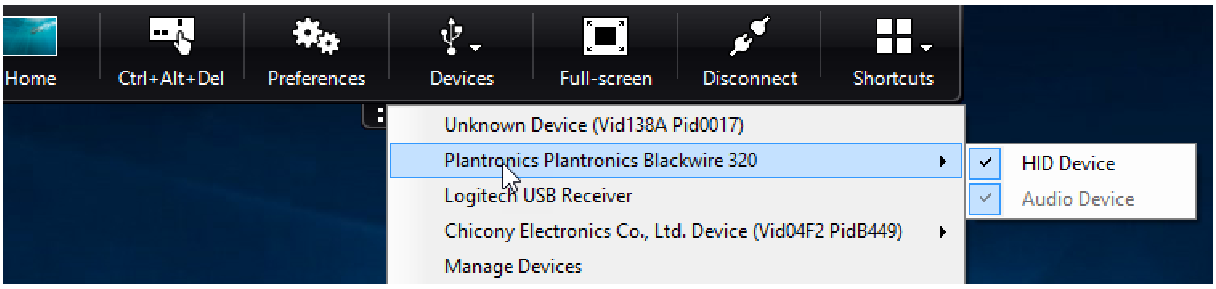
Configuring composite USB redirection:

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. Click **Apply** Click **OK** to save the policy.

To allow or deny an interface:

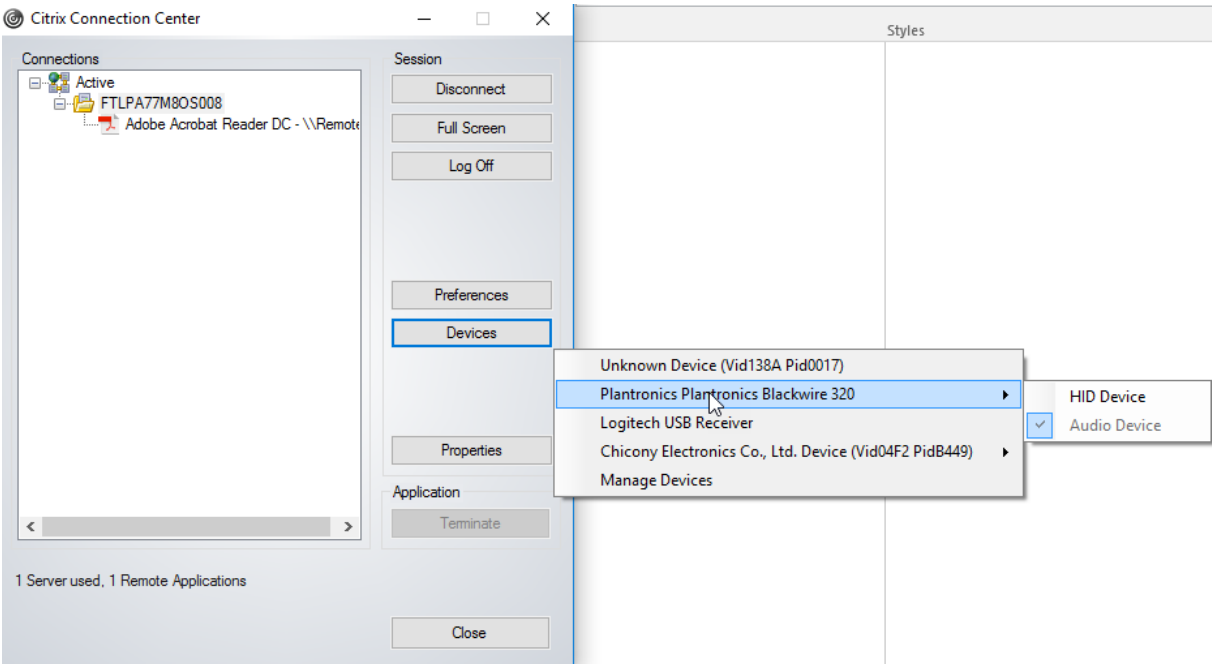
1. Open the Citrix Workspace app Group Policy Object administrative template by running gpedit.msc.
2. Under the **User Configuration** node, go to **Administrative Templates** > **Citrix Components** > **Citrix Workspace** > **Remoting client devices** > **Generic USB Remoting**.
3. Select **USB Device Rules** policy.
4. Select **Enabled**.
5. In the **USB Device Rules** text box, add the USB device that you want to allow or deny.
   For example, `ALLOW: vid=047F pid= C039 split=01 intf=00,03` - allows 00 and 03 interface and restrict others.
6. Click **Apply** and **OK**.

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**.


Home
Ctrl+Alt+Del
Preferences
Devices
Full-screen
Disconnect
Shortcuts
Unknown Device (Vid138A Pid0017)
Plantronics Plantronics Blackwire 320
Logitech USB Receiver
Chicony Electronics Co., Ltd. Device (Vid04F2 PidB449)
Manage Devices
HID Device
Audio Device

> **Note:**
>
> When you split a composite USB device for generic USB redirection, you must select the device from Desktop Viewer or Connection Center to redirect the device.

In an application session, split USB devices are displayed in the **Connection Center**.



The table below provides details on the behavior scenarios when a USB interface is allowed or denied.

To allow an interface:

Split	Interface	Action
TRUE	Valid number 0 -n	Allow specified interface
TRUE	Invalid number	Allow all interfaces
FALSE	Any value	Allow Generic USB of parent device

Split	Interface	Action
Not specified	Any value	Allow Generic USB of parent device

For example, SplitDevices- *true* indicates that all devices split.

To deny an interface:

Split	Interface	Action
TRUE	Valid number 0 -n	Deny specified interface
TRUE	Invalid number	Deny all interfaces
FALSE	Any value	Deny Generic USB of parent device
Not specified	Any value	Deny Generic USB of parent device

For example, SplitDevices- *false* indicates that devices are not split with specified interface number.

Example: *MyPlantronics* headset

Interface number:

- Audio Interface Class -0
- HID Interface Class-3

Sample rules used for *MyPlantronics* headset:

- ALLOW: `vid=047F pid= C039 split=01 intf=00,03 /Allowed 00 and 03 interface, restrict others`
- DENY: `vid=047F pid= C039 split=01 intf=00,03 / deny 00 and 03`

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.

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. This means that session scaling follows the operating system resolution.

You can configure DPI scaling using the following options:

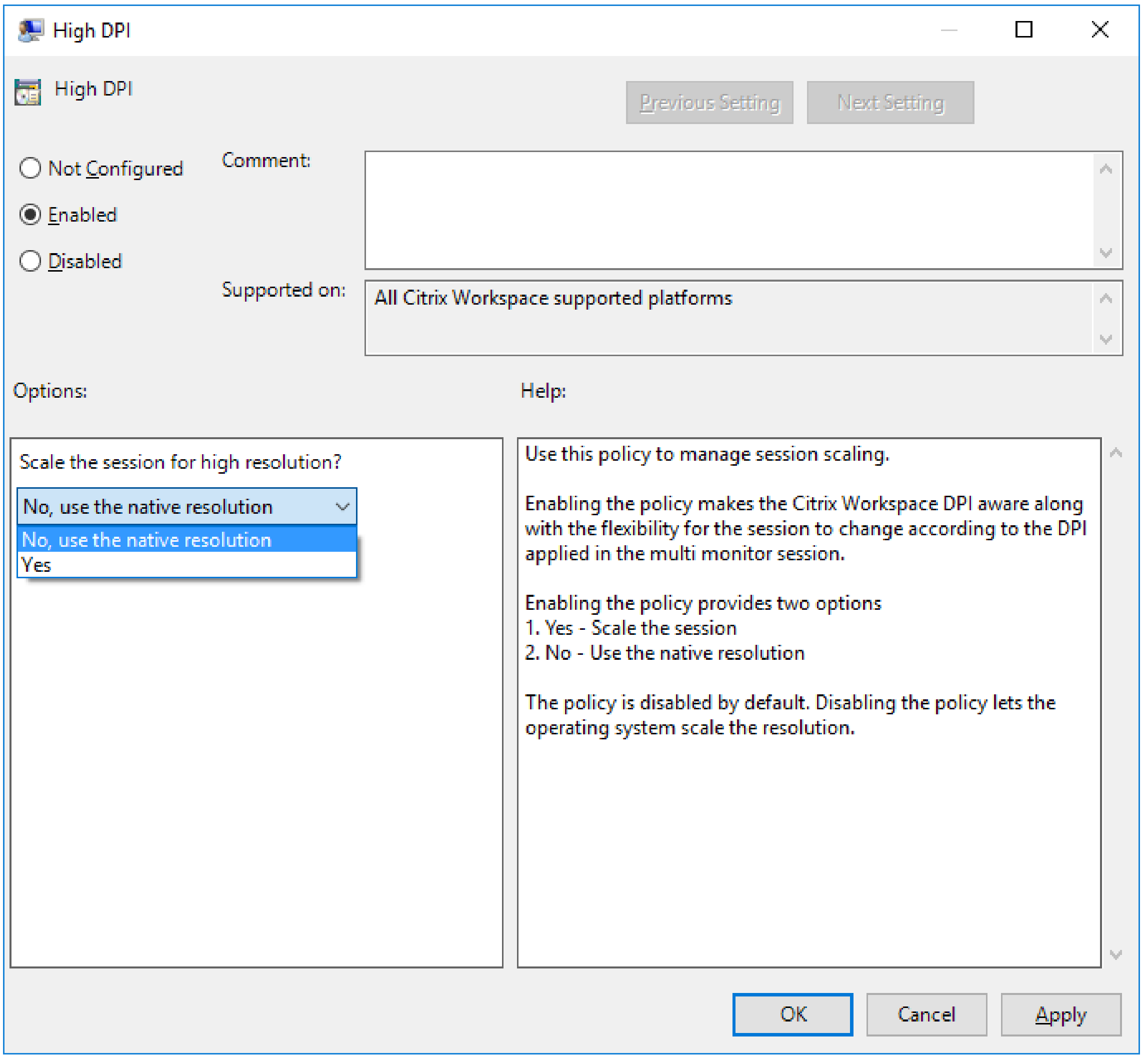
1. Group Policy Object (GPO) administrative template (per-machine configuration)
2. Advanced Preferences (per-user configuration)

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 **High DPI** policy.



All Citrix Workspace supported platforms

Scale the session for high resolution?

No, use the native resolution

No, use the native resolution
Yes

Use this policy to manage session scaling.

Enabling the policy makes the Citrix Workspace DPI aware along with the flexibility for the session to change according to the DPI applied in the multi monitor session.

Enabling the policy provides two options
1. Yes - Scale the session
2. No - Use the native resolution

The policy is disabled by default. Disabling the policy lets the operating system scale the resolution.

4. Select from one of the following options:

   a) Yes - Indicates that high DPI is applied in a session.
   b) No, use the native resolution - Indicates that the resolution is set by the operating system.

5. Click **Apply and OK**.

6. From the command line, run the `gpupdate /force` command to apply the changes.

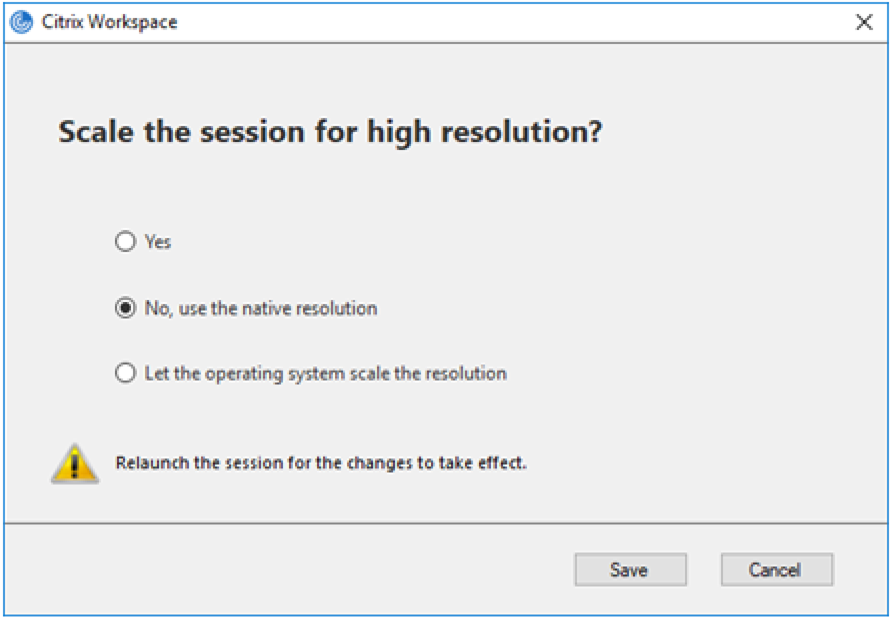
Configure DPI scaling using the graphical user interface:

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

1. Right-click Citrix Workspace app icon from the notification area.

2. Select **Advanced Preferences** and click **DPI settings**.

   The DPI settings dialog appears.



Citrix Workspace

Scale the session for high resolution?

○ Yes

● No, use the native resolution

○ Let the operating system scale the resolution

Relaunch the session for the changes to take effect.

3. Select one of the following options:

   a) Yes - Indicates that 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. This corresponds to the UI setting Yes, or the High DPI policy set to Enabled in the GPO policy. This setting works well for mixed DPI scenarios when connecting to modern VDAs. This is the only way to scale seamless sessions. Scaling might cause 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 do not work 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. This corresponds to the UI setting "No"and the HighDPI policy is set to Enabled in the GPO. This setting does not 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. This 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. This lets the Windows Operating system handle 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 Windows 10 Operating system.
This setting is recommended for users on Windows 7 endpoints, or those 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 that applies to the remote desktop and to virtually split a single client monitor into up to eight monitors on the remote desktop. You can configure the virtual monitors on 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 percentages of the client monitor resolution.

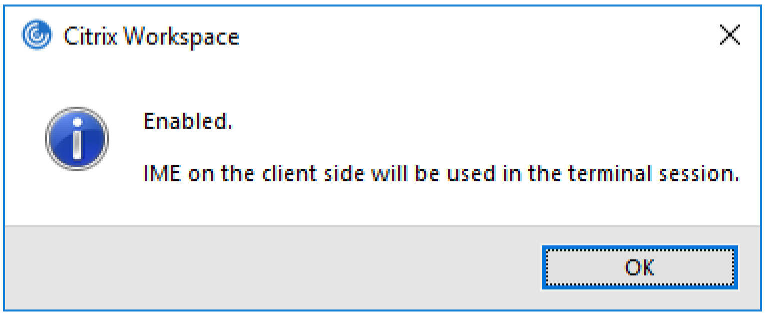
You can set a DPI for the virtual monitors that is used for DPI scaling or DPI matching. After applying a virtual monitor layout, resize or reconnect the session.

This configuration applies only to full-screen sessions, 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)

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`
  .

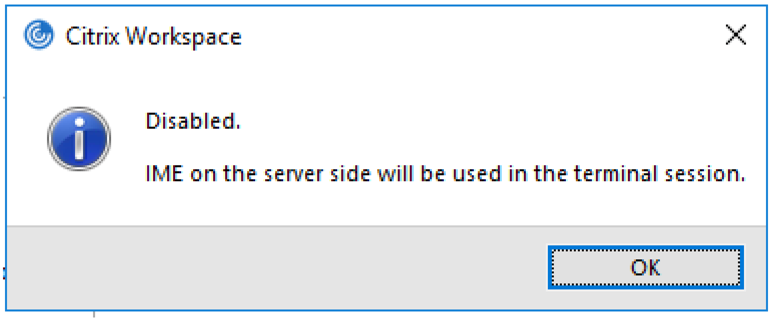
  

  Citrix Workspace

  Enabled.

  IME on the client side will be used in the terminal session.

- 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`.

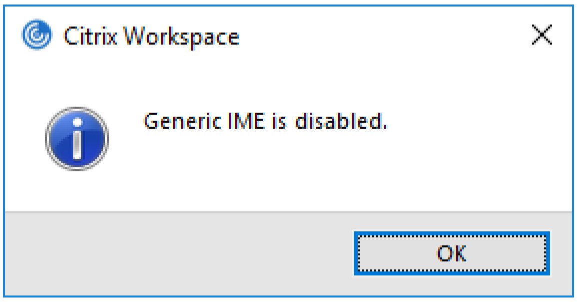
  Citrix Workspace

  Disabled.

  IME on the server side will be used in the terminal session.

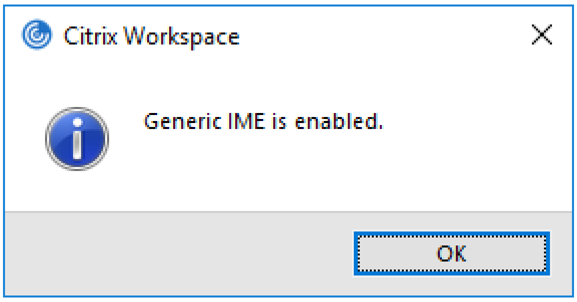
> **Note:**
>
> You can use the command-line switch `wfica32.exe /localime:on` to enable both generic client IME and keyboard layout synchronization.

- 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 keyboard layout synchronization settings.



Generic IME is disabled.

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.



Generic IME is enabled.

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.

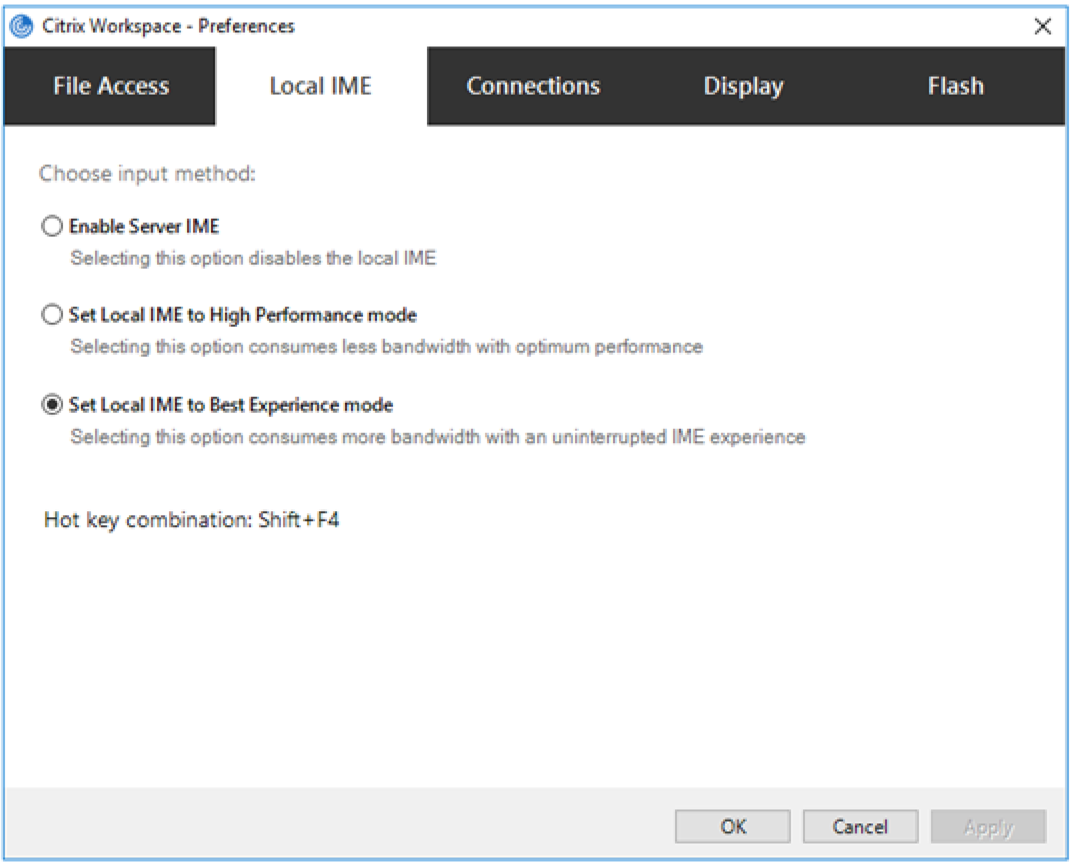
Configure generic client IME using the graphical user interface:

Generic client IME requires VDA Version 7.13 or later.

Generic client IME feature 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. In an active application session, right-click the Citrix Workspace app icon in the notification area and select **Connection Center**.
2. Select **Preferences** and **Local IME**.



Choose input method:

○ Enable Server IME
Selecting this option disables the local IME

○ Set Local IME to High Performance mode
Selecting this option consumes less bandwidth with optimum performance

● Set Local IME to Best Experience mode
Selecting this option consumes more bandwidth with an uninterrupted IME experience

Hot key combination: Shift+F4

The options below 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 change in settings is applied only for the current session.

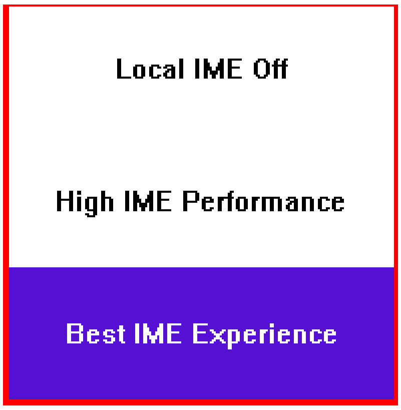
Enabling hotkey configuration using a registry editor:

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_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Citrix\ICA Client\Engine\Lockdown Profiles\All Regions\Lockdown\Client Engine\Hot Keys`.

Select **AllowHotKey** and change the default value to 1.



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 do this, click **Security** and uncheck **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. To benefit from this feature, it must be supported and enabled on both the VDA and Citrix Workspace app. If the GPU on the endpoint does not support H.265 decoding using the DXVA interface, the H265 Decoding for graphics policy settings is ignored and the session falls back to using the 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:

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 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 is ignored and the feature does not work.
> - Run the HDX Monitor 3.x tool to identify if H.265 video encoder is enabled within the sessions. For more information about HDX Monitor 3.x tool, see Knowledge Center article CTX135817.

Keyboard layout and language bar

Keyboard layout

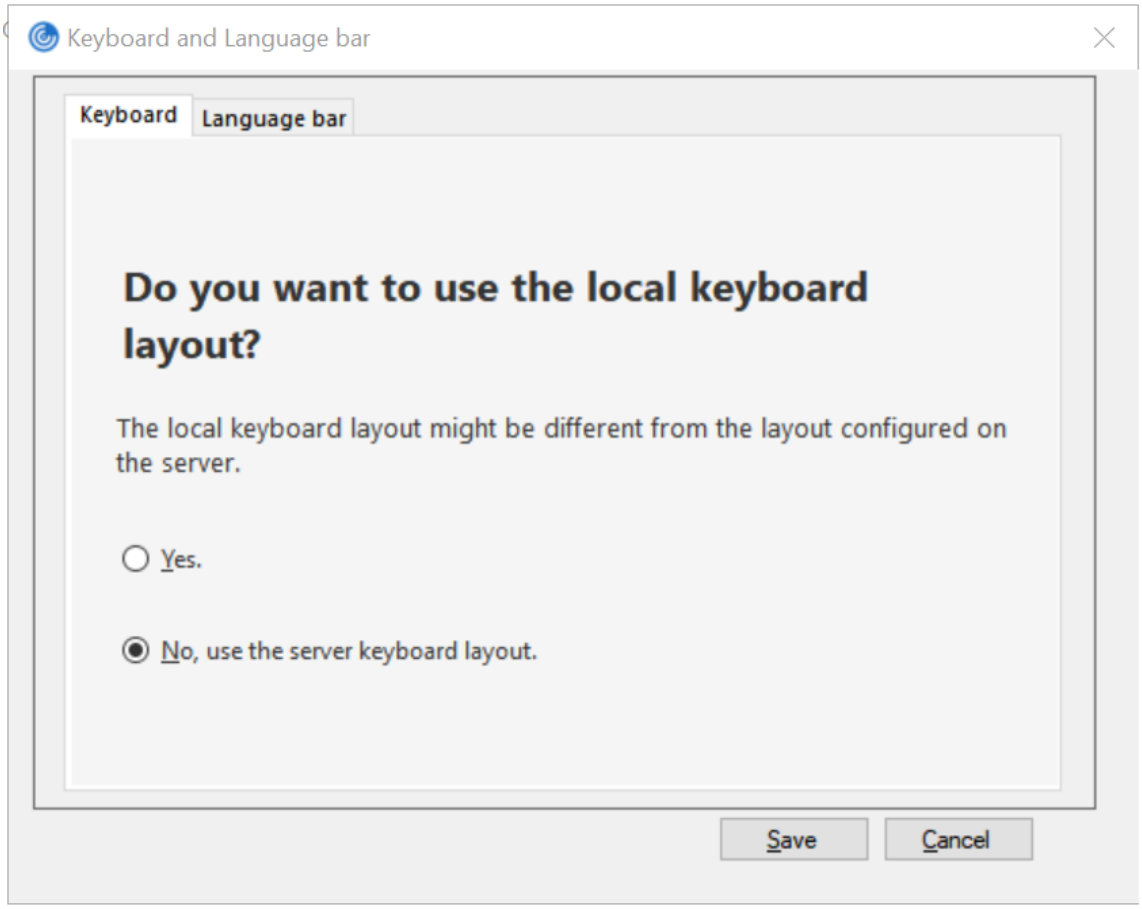
> **Note:**
>
> You can hide all or part of the Advanced Preferences sheet available from the Citrix Workspace app icon in the notification area. For more information, see Advanced Preferences sheet.

Keyboard layout synchronization enables users to switch among preferred keyboard layouts on the client device. This feature is disabled by default.

To enable keyboard layout synchronization:

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.

   Do you want to use the local keyboard layout?

   The local keyboard layout might be different from the layout configured on the server.

   ○ Yes.

   ● No, use the server keyboard layout.

2. Select from one of the following options:

   - Yes - Indicates that the local keyboard layout is used in a session.
   - No, use the server keyboard - Indicates that the keyboard layout used on the VDA is applied in a session. This option sets the local keyboard layout feature to disabled.

3. Click **Save**.

You can also enable and disable keyboard layout synchronization using the command line by running `wfica32:exe /localime:on` or `wfica32:exe /localime:off` from the Citrix Workspace app for Windows installation folder `C:\Program files (x86)\Citrix\ICA Client`.

Using the local 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 local 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.

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 Registry Editor can be solved. Use 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 which is not supported on the server, the keyboard layout synchronization feature 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.
- This feature is disabled in Windows Server 2016 due to a third-party issue which might introduce performance risk. The feature can be enabled with a registry setting on the VDA: in `HKEY_LOCAL_MACHINE\Software\Citrix\ICA\IcaIme`, add a new key called **DisableKeyboardSync** and set the value to 0.

Language bar

The language bar displays the preferred input language in a session. In earlier releases, you could change this setting using only the registry keys on the VDA. Starting with Citrix Receiver for Windows Version 4.11, you can change the settings using the **Advanced Preferences** dialog. The language bar appears in a session by default.

> **Note:**
>
> This feature is available in sessions running on VDA 7.17 and later.

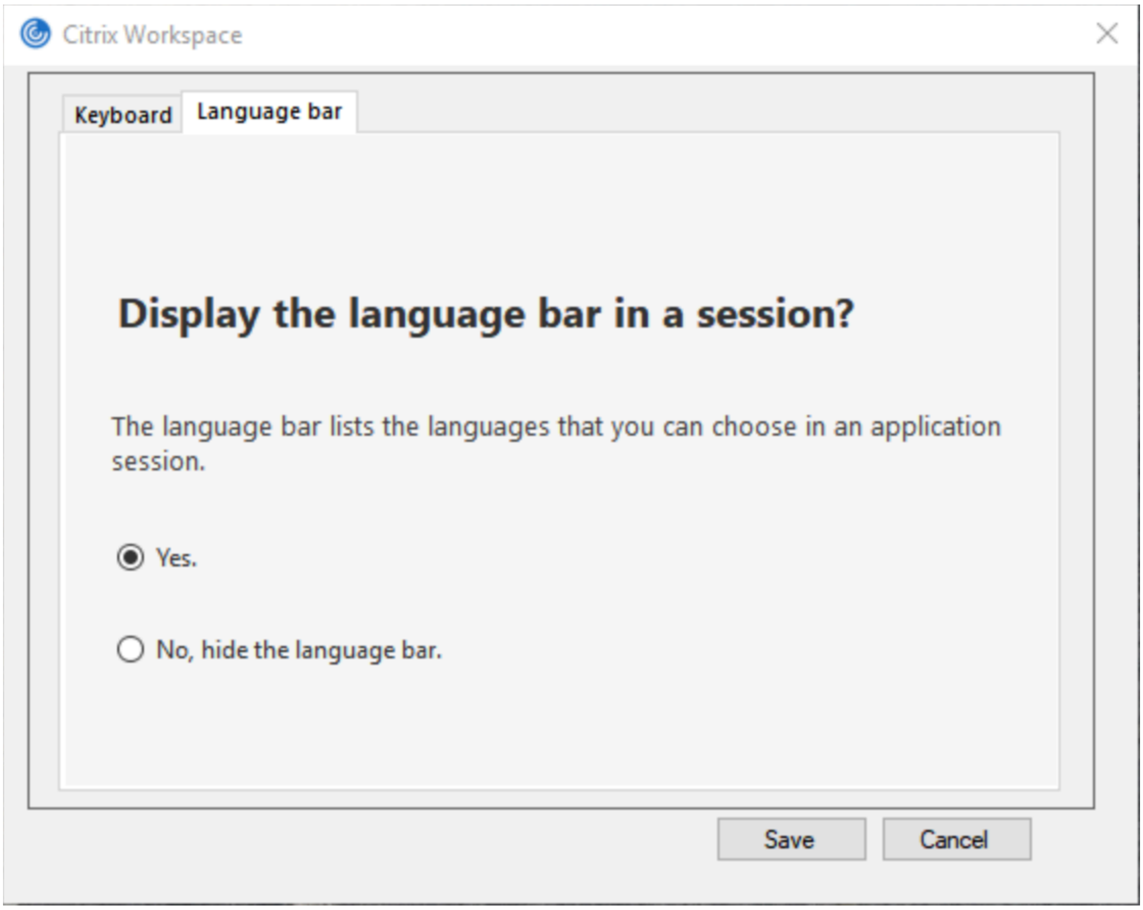
Configure showing or hiding the remote language bar:

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.



Display the language bar in a session?

The language bar lists the languages that you can choose in an application session.

● Yes.

○ No, hide the language bar.

> **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 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/high-speed LAN environments. This allows these devices to interact with packages, such as 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 may have a network interface card 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 network interface cards
- 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 Citrix Virtual Apps session:

- Bluetooth dongles
- Integrated network interface cards
- USB hubs
- USB graphics adapters
- Audio devices
- Mass storage devices

How USB support works:

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 device is denied by the default policy, 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 decide which USB devices are remoted to the virtual desktop by selecting devices from the list 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, which you configure through the Citrix Workspace app for Windows policy **Remoting client devices** > **Client drive mapping**. When this policy is applied, the drives on the user device are automatically mapped 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 both Generic USB and the Client drive mapping policies are enabled and a mass storage device is inserted 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:

Different classes of USB device are allowed by the default USB policy rules.

Although they are on this list, some classes are only available for remoting in virtual apps and desktops sessions after additional configuration. These are noted below.

- **Audio (Class 01)**- Includes audio input devices (microphones), audio output devices, and MIDI controllers. Modern audio devices generally use isochronous transfers, which are supported by

XenDesktop® 4 or later. Audio (Class01) is not applicable to Citrix Virtual Apps because these devices are not available for remoting in Citrix Virtual Apps using USB support.

> **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 may also appear as mass storage devices and it may be possible to configure a camera to use either class, through 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 may 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

  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 covers devices that are used to manipulate video or video-related material, 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, which are supported by XenDesktop 4 or later. 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 these usually appear as vendor-specific (class ff).

USB devices classes denied by default

The following different classes of USB device are denied by the default USB policy rules.

- Communications and CDC Control (Classes 02 and 0a). The default USB policy does not allow these devices, because one of the devices may 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 does not allow USB keyboards (class 03, subclass 01, protocol 1), or USB mice (class 03, subclass 01, protocol 2). This is because most keyboards and mice are handled appropriately without USB support and it is normally necessary to use these devices locally as well remotely when connecting 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.

  Smart card readers are accessed using smart card remoting and do not require USB support.

- Wireless Controller (Class e0). Some of these devices may 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 may 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 may be providing critical network access. The default USB policy does not allow these devices. However, there may be particular devices to which it is appropriate to provide access using USB support.

Update the list of USB devices available for remoting

You can update the range of USB devices available for remoting to desktops by editing the Citrix Workspace for Windows template file. This allows you to make changes to the Citrix Workspace for Windows using Group Policy. The file is located 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 may require you to reinstall your operating system. Citrix cannot guarantee that problems resulting from the incorrect use of Registry Editor can be solved. Use 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 latest template files to the local GPO. For more information on adding template files to the local GPO, see Group Policy Object administrative template. In case of an 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 cmd prompt in administrator mode.
6. Run the below command
   `gpupdate /force`.

vPrefer launch

In earlier releases, you could 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 is hosting 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) in preference to launching 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 installation path of the application in the Windows registry on the VDA and, 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 installed on the VDA, the hosted application is launched. For more information on how the local launch is handled on StoreFront, 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.

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. In case of 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** and from the **Allow apps** drop-down, 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) and 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 such as Notepad, Calculator etc.
    - **Allow network apps**: This option launches the instance of an app that is published on a shared network.

5. Click **Apply** and **OK**.
6. Restart the session for the changes to take effect.

Limitation:

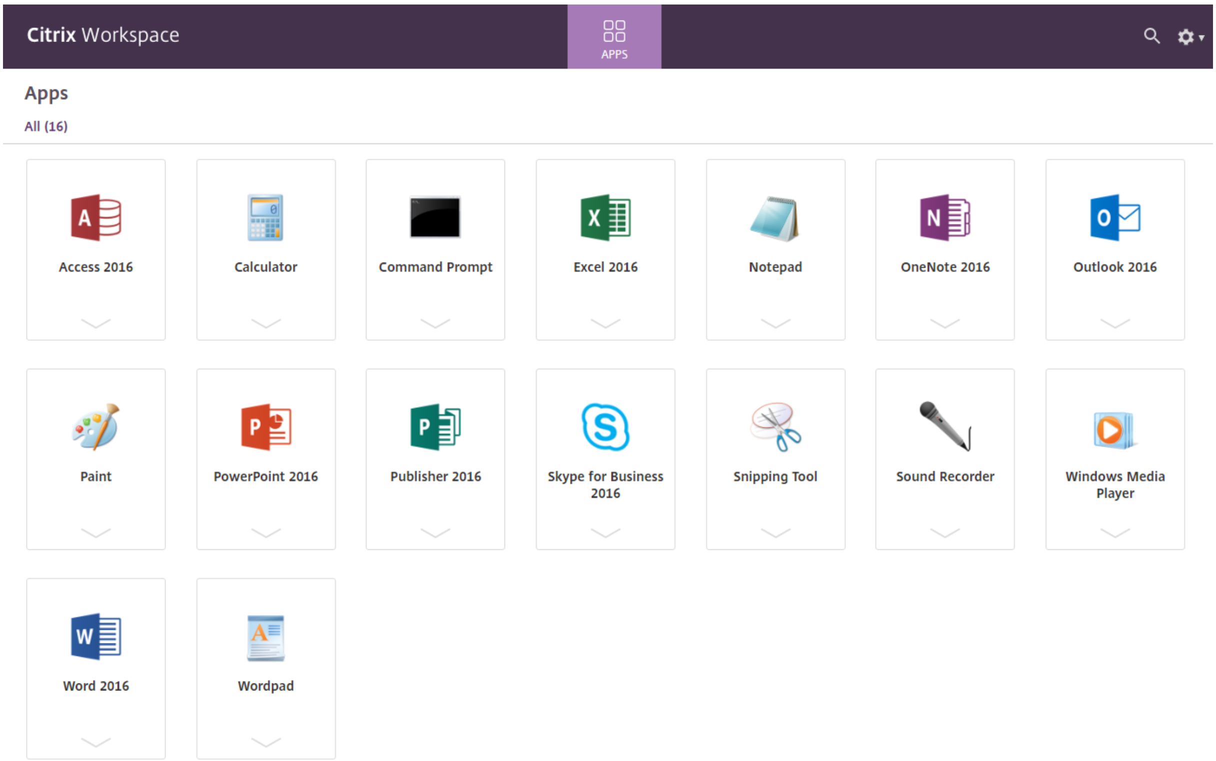
- Workspace for Web does not support this feature.

Workspace configuration

Citrix Workspace app for Windows supports configuring Workspaces for subscribers, who might be using one or more services available from Citrix Cloud.

Citrix Workspace app will intelligently display 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.

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 may 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 by filtering access to specific websites and website categories.

Citrix Workspace app for Windows support the use of SaaS apps using the Access Control Service. 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.

Prerequisites:

- The SaaS application must support SAML 2.0 authentication to be able to apply the single sign-on feature.
- The **Enable enhanced security** option must be enabled on the Access Control Service so that the Citrix Enterprise Browser (formerly Citrix Workspace Browser) is used while rendering a SaaS application. If this is option is not enabled, SaaS apps are launched using the default browser as set on the client.

> **Note:**
>
> Citrix Workspace app aggregates the apps and desktops that are published both from on-premises and cloud environments for a unified user experience.

Citrix Workspace app includes an embedded Citrix Secure Browser to launch the SaaS apps. The Chromium embedded framework on which Citrix Secure Browser is built is on Version 70. This results in a better user experience when accessing secure SaaS apps.

> **Note:**
>
> - In case of Workspace for Web, SaaS apps are launched only in the default browser as set on the client and not in the Citrix Secure Browser.
> - The user experience between an ICA® session app and a secure SaaS app might vary.

The Citrix Secure Browser supports operations such as toolbar, clipboard, Print, Download, and Watermark. These operations are applied in Citrix Workspace app as defined in the policy configuration on the Access Control Service.

Operations that you can perform using the Citrix Secure Browser:

Toolbar - When the toolbar option is enabled on an app, you can view the Back, Forward, and Refresh options in the launched app. The toolbar also displays an ellipsis that includes Clipboard operations.

Clipboard - When the clipboard access is enabled on an app, you can use the Cut, Copy, and Paste options that appear in the toolbar in the launched app. When the option is disabled, the Cut, Copy, and Paste options are grayed out.

Print - You can run a print command in the launched app if the print option is enabled. When disabled, the print option does not appear in the launched app.

Navigation - The next and the previous icon appear in the toolbar in the launched app if the navigation option is enabled.

Download - You can download files from the launched app if the download option is enabled. Right-click on the launched app and select **Save as**. Browse to the desired location and click **Download**.

> **Note:**
>
> When you download a file, a progress bar is not displayed to indicate the status of the download. The download, however, is successful.

Watermark - When the watermark option is enabled, a watermark containing the user name and the IP address of the client machine appears in the launched app. The watermark is semi-transparent and cannot be edited to display any other information.

Configuring cache using the GPO:

When multiple users use the same device to log in to access the Secure SaaS apps, the cache gets carried forward to the subsequent user, thereby sharing browsing information across users.

To address this issue, Citrix Workspace app introduces a new Group Policy Object (GPO) administrative policy. This policy will disallow the storing of the browser cache on the local device.

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** > **Citrix Secure browser**.
3. Select the **Cache** policy.
   Note: By default, this policy is set to **Enabled**.
4. To disable it, select **Disabled** and click **Apply** and **OK**.
5. Restart Citrix Workspace app for the change to take effect.

Limitations:

1. When you launch a published app with print option enabled and download disabled, and give a print command on a launched app, you might be able to save the PDF even when the download functionality is restricted. 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 Workspace configuration, see Workspace configuration in Citrix Cloud.

PDF Printing

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 are not supported on the Microsoft Edge browser.

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 is 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.

The Windows 10 VDA detects the presence of a keyboard or a mouse on a touch-enabled client device 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 apps you start open in a full screen.
- The taskbar contains a Back button.
- Icons are removed from the taskbar.

Desktop mode offers the traditional user interface where you interact in the same manner as using a PC with a keyboard and mouse.

> **Note:**
>
> Workspace for Web does not support Windows Continuum feature.

Relative mouse

Relative mouse support provides an option to interpret the mouse position in a relative rather than an absolute manner. This capability is required for applications that demand relative mouse input rather than absolute.

> **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.

You can control the availability of the feature on a per-user and a per-machine basis using the registry as follows:

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 in these 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 when it was created.

In case of StoreFront customers, default.ica file is typically located at `C:\inetpub\wwwroot\Citrix\<Storename>\App_Data\default.ica`, where storename is the name specified for the store when it was created.

2. Add a new key by name RelativeMouse in the WFClient section, with its value set 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 takes 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 relative mouse from the Desktop Viewer applies the feature to per-session only.

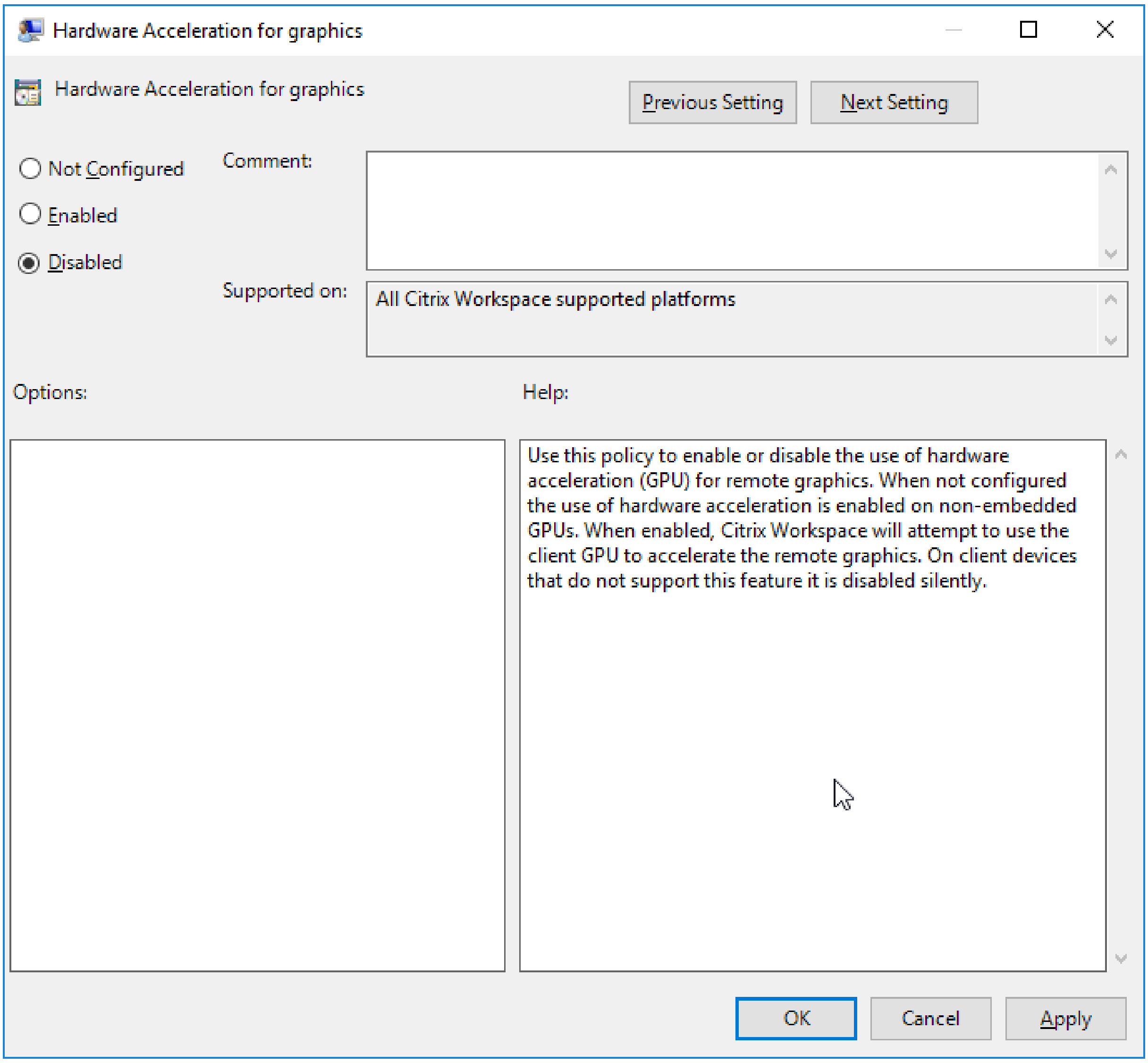
Hardware decoding

When using Citrix Workspace app (with HDX engine 14.4), the GPU can be used for H.264 decoding wherever it is 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.

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**.



Supported on: All Citrix Workspace supported platforms

Help: Use this policy to enable or disable the use of hardware acceleration (GPU) for remote graphics. When not configured the use of hardware acceleration is enabled on non-embedded GPUs. When enabled, Citrix Workspace will attempt to use the client GPU to accelerate the remote graphics. On client devices that do not support this feature it is disabled silently.

To validate if the policy was applied and hardware acceleration is being used for an active ICA session, look for 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** should be 2. If the value is 1, that means CPU-based decoding is being used.

When using the hardware decoding feature, consider the following limitations:

- If the client has two GPU's and if one of the monitors is active on the second GPU, CPU decoding will be used.
- When connecting to a Citrix Virtual Apps server running on Windows Server 2008 R2, Citrix recommends that you do not to 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. Locally installed microphones can be used 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.

Multi-monitor support

You can use up to eight monitors with Citrix Workspace app for Windows.

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 subsequently, 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, ensure the following:

- The user device is configured to support multiple monitors.
- The operating system must be able to 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 have 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.

Ensure that the setting is large enough (in kilobytes) to provide sufficient graphic memory. If this setting is not 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 information about 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 make changes to 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 cannot accurately detect the mode of the device, and the on-screen keyboard may appear when you do not 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.

> **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 3 different modes as given below:

- **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 desired options.
5. Restart the Citrix Workspace app session for the changes to take effect.

Support for 32-bit color icons:

Citrix Workspace app supports 32-bit high color icons and automatically selects the color depth for applications visible in the **Citrix Connection Center** dialog, the Start menu, and task bar to provide for seamless applications.

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

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 desired 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 have different corporate needs. Your requirements for the way users access virtual desktops may vary from user to user and may vary as your corporate needs evolve. The user experience of connecting to virtual desktops and the extent of user involvement in configuring the connections depend on how you set up Citrix Workspace app for Windows.

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 with 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 cannot change the screen resolution using Windows Control Panel.

Keyboard input in Desktop Viewer

In Desktop Viewer sessions, **Windows logo** key+L is directed to the local computer.

Ctrl+Alt+Delete is directed to the local computer.

Key presses that activate Sticky Keys, Filter Keys, and Toggle Keys (Microsoft accessibility features) 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.

Hotkey sequences are key combinations designed by Citrix. For example, the Ctrl+F1 sequence reproduces Ctrl+Alt+Delete, and Shift+F2 switches applications between full-screen and windowed mode. You cannot use hotkey sequences with virtual desktops displayed in the Desktop Viewer (that is, with virtual apps and desktops sessions), but you can use them with published applications (that is, with Citrix Virtual Apps sessions).

Virtual desktops

From within a desktop session, users cannot connect to the same virtual desktop. Attempting to do so will disconnect the existing desktop session. Therefore, Citrix recommends:

- Administrators should not configure the clients on a desktop to point to a site that publishes the same desktop
- Users should not browse to a site that hosts the same desktop if the site is configured to automatically reconnect users to existing sessions
- Users should not browse to a site that hosts the same desktop and try to launch it

Be aware that a user who logs on locally to a computer that is acting as a virtual desktop blocks connection to that desktop.

If your users connect to virtual applications (published with Citrix Virtual Apps) from within a virtual desktop and your organization has a separate Citrix Virtual Apps administrator, Citrix recommends working with them to define device mapping such that 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, create a REG_DWORD value SI INACTIVE MS in HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\ CLIENT\Engine\. The REG_DWORD value can be set to 4 if you want the status indicator to disappear sooner.

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.

Additional information

Citrix will handle your data in accordance with the terms of your contract with Citrix, and protect it as specified in the Citrix Services Security Exhibit available on the Citrix Trust Center.

Citrix also uses Google Analytics to collect certain data from Citrix Workspace app as part of CEIP. Please review how Google handles data collected for Google Analytics.

You can turn off sending CEIP data to Citrix and Google Analytics (except for the two data elements collected for Google Analytics indicated by an * in the second table below) 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**.

Alternatively, you can 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** in the data collection dialog or set the `Enable_CEIP` key to `False`, if you would like to disable sending the final two CEIP data elements collected by Google Analytics (that is, Operating System version & Citrix Workspace app version) navigate to the following registry entry and set the value as suggested:

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:

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

Authenticate

September 13, 2025

Secure the connections between Citrix Workspace app and the published resources to maximize the security. You can configure the following types of authentication:

- Domain pass-through
- Smart card
- Kerberos pass-through

Domain pass-through authentication

Single sign-on lets you authenticate and use the virtual apps and desktops without having to reauthenticate again.

Logging in to Citrix Workspace app allows your credentials and enumerated resources to be passed through to StoreFront.

In earlier releases, when using Google Chrome, Microsoft Edge or Mozilla FireFox, you can launch single sign-on sessions even if the feature was not enabled.

Starting with Version 1905, all web browsers require you to configure single sign-on using the Group Policy Object administrative template. For more information about configuring single sign-on using Group Policy Object 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
- Graphical user interface(GUI)

Configure single sign-on during fresh installation

Configuring single sign-on during fresh installation:

1. Configuration on StoreFront or the Web Interface.
2. Configure XML trust services on the Delivery Controller.
3. Modify Internet Explorer settings.
4. Install Citrix Workspace app with single sign-on.

Configure single sign-on on StoreFront or Web Interface

Depending on the type of Citrix Virtual Apps and Desktops deployment, single sign-on can be configured on StoreFront or the Web Interface using the Management Console.

Use the table below for different use case and its respective configuration:

Use case	Configuration details	Additional information
Configured SSON on StoreFront or Web Interface	Launch Citrix Studio, go to **Store** > **Manage Authentication methods** > enable **Domain pass-through**.	When Single Sign-on is not configured, Citrix Workspace app automatically switches the authentication method from **Domain pass-through** to **Username and Password**, if available.
When Workspace for Web is required	Launch **Store** > **Workspace for Websites** > **Manage Authentication methods** > enable **Domain pass-through**.	When Single Sign-on is not configured, Citrix Workspace app automatically switches the authentication method from **Domain pass-through** to **Username and Password**, if available.
When StoreFront is not configured	If Web Interface is configured on the VDA, launch XenApp Services Sites > **Authentication Methods** > enable **Pass-through**.	When Single Sign-on is not configured, Citrix Workspace app automatically switches the authentication method from **Pass-through** to **Explicit**, 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**.
3. Select **Single Sign-on for Citrix Gateway** policy.
4. Select **Enabled**.
5. Click **Apply** and **OK**.
6. 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 (formerly Citrix Virtual Apps and Desktops service) , run the following PowerShell command as an administrator on the Delivery Controller:

```
asnp Citrix* Set-BrokerSite -TrustRequestsSentToTheXmlServicePort
$True
```

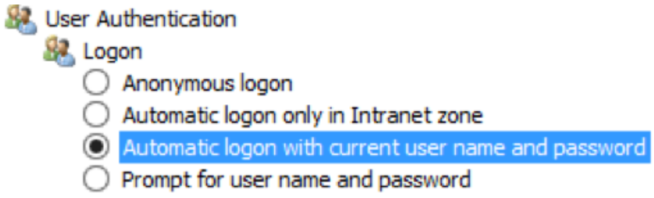
Modify the Internet Explorer settings

1. Add the StoreFront server to the list of trusted sites using Internet Explorer. To do this:

   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 or Web Interface FQDN with the appropriate HTTP or HTTPS protocols.
   e) Click **Apply** and **OK**.

2. Modify the **User Authentication** settings in **Internet Explorer**. To do this:

   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**.



User Authentication
Logon
○ Anonymous logon
○ Automatic logon only in Intranet zone
● Automatic logon with current user name and password
○ Prompt for user name and password

   a) Click **Apply** and **OK**.

Configure single sign-on using the command-line interface

Install Citrix Workspace app for Windows with the `/includeSSON` switch and restart Citrix Workspace app for the changes to take effect.

> **Note:**
>
> If Citrix Workspace app for Windows is installed without the single sign-on component, upgrading to the latest version of Citrix Workspace app with the `/includeSSON` switch is not supported.

Configure single sign-on using the graphical user interface

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 using Citrix Workspace app without providing user credentials.

Configure single sign-on on Citrix 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 password** policy and set it to **Enabled**.
4. Click **Enable pass-through authentication**. This option allows 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 single sign-on is enabled by launching the **Task Manager** and check if the `ssonsvr.exe` process is running.

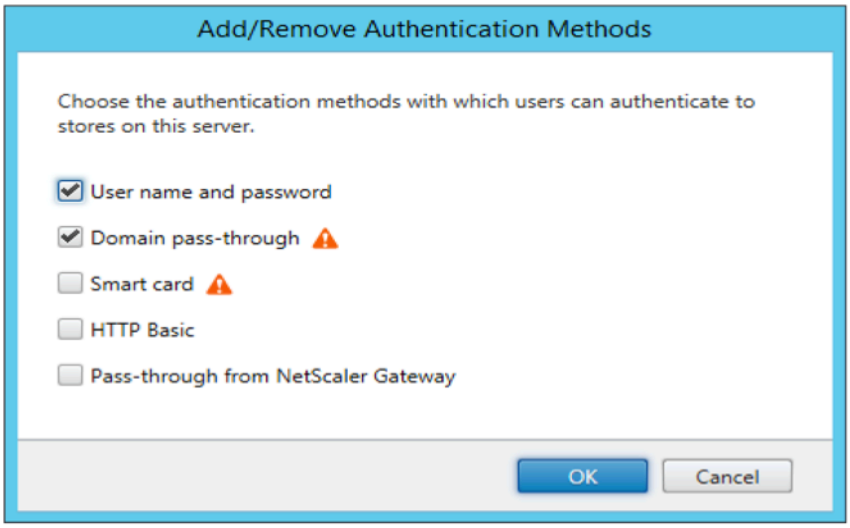
Configure single sign-on using Active Directory

You can configure single sign-on authentication using the Active Directory. You do not need to use deployment tools, such as Microsoft System Center Configuration Manager in this case.

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 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 `icaclient.adm` file.
6. After adding the `icaclient.adm` template, go to **Computer Configuration** > **Administrative Templates** > **Citrix Components** > **Citrix Workspace** > **User authentication**.
7. Select the **Local user name** 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 and Web Interface

StoreFront configuration Open **Citrix Studio** on the StoreFront server and select **Authentication > Add /Remove Authentication Methods**. Select **Domain pass-through**.



Add/Remove Authentication Methods

Choose the authentication methods with which users can authenticate to stores on this server.

☑ User name and password

☑ Domain pass-through ⚠

□ Smart card ⚠

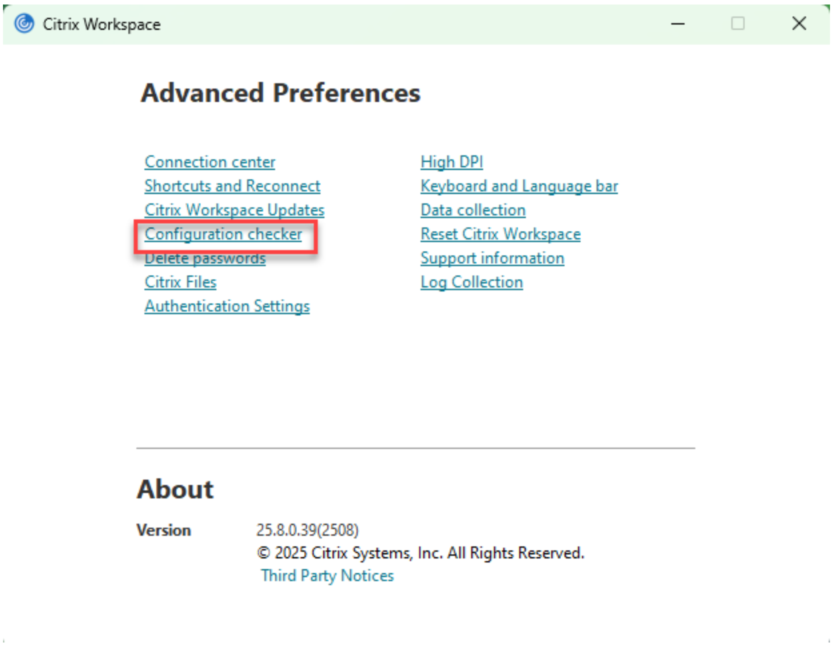
□ HTTP Basic

□ Pass-through from NetScaler Gateway

Configuration Checker

Configuration Checker lets you run a test to ensure that 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.



Advanced Preferences

About

Version 25.8.0.39(2508)

© 2025 Citrix Systems, Inc. All Rights Reserved.

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.
   - 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 is not 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.

The user gets more information about each checkpoint and the corresponding results.

The following tests are performed:

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: Ensure 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 Web Interface/StoreFront.

> **Note:**
>
> - Test results are not applicable on Workspace for Web configurations.
> - In a multi-store setup, 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 Group Policy Object 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.
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 the VDA.

Beacon test Beacon checker is part of **Configuration Checke** utility. It allows you to perform a beacon test to confirm if the beacon (ping.citrix.com) is reachable. This test helps to eliminate one of the many possible causes for slow resource enumeration, that is 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 **Beacon checker** 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 is able to contact the beacon intermittently.

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).

Kerberos authenticates without passwords for Citrix Workspace app. Thereby, preventing 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.
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 is not used, Citrix Workspace app authenticates to StoreFront using the smart card credentials.

3. The HDX engine 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, ensure that your 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 must also be 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 ensure that Kerberos is used, disable any non-Kerberos IWA options on the domain.
- Kerberos log on is not available for Remote Desktop Services connections that are configured to use either Basic authentication, always use specified logon information, or always prompt for a password.

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

Domain pass-through authentication with Kerberos for use with smart cards

See the smart card information present in the Secure your deployment section in the Citrix Virtual Apps and Desktops documentation before continuing.

When you install Citrix Workspace app for Windows, include the following command-line option:

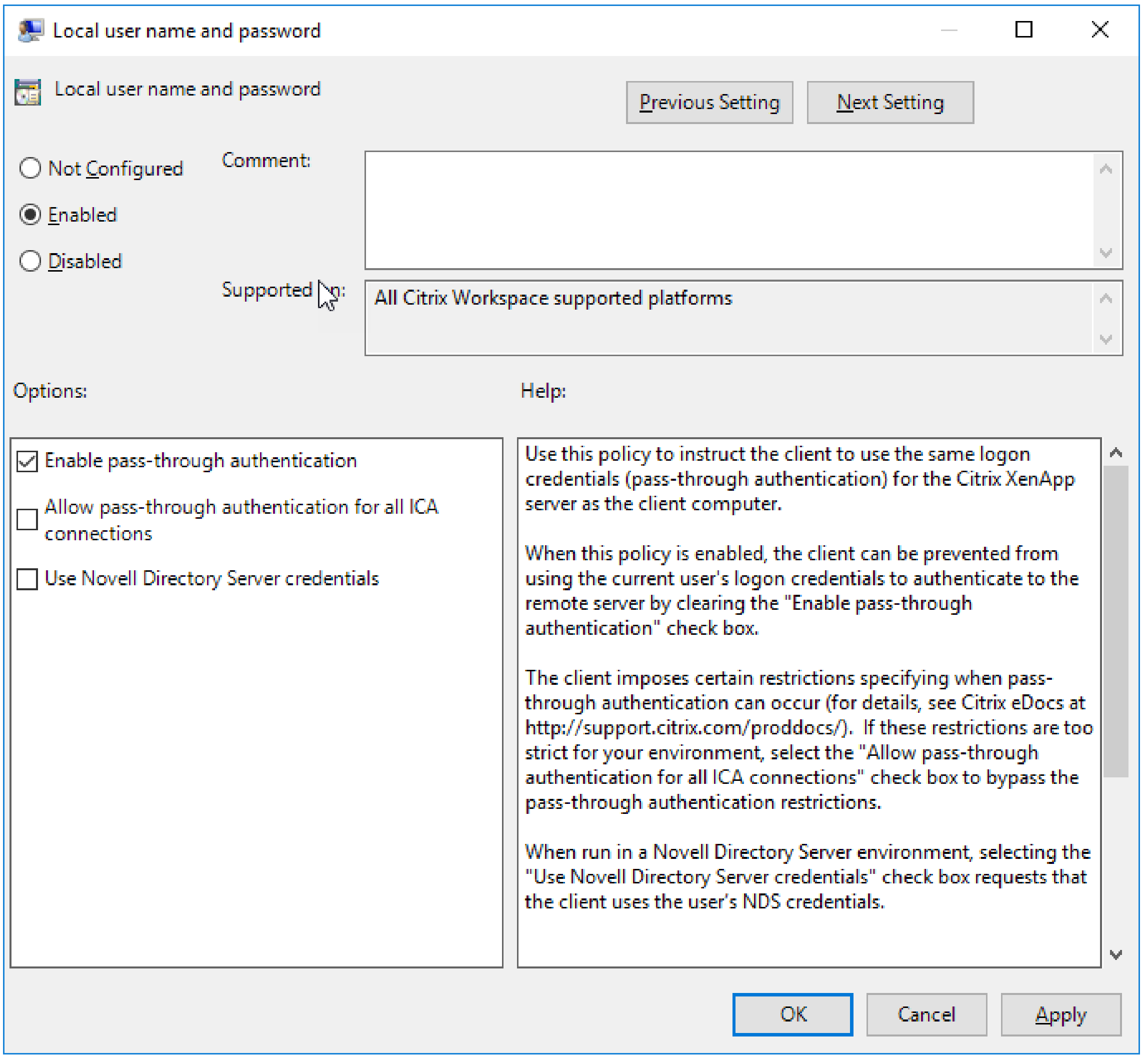
- `/includeSSON`

  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 component stores the smart card PIN, which is 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 obtains 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.



Local user name and password

Local user name and password

○ Not Configured
● Enabled
○ Disabled

Comment:

Supported on: All Citrix Workspace supported platforms

Options:

☑ Enable pass-through authentication
□ Allow pass-through authentication for all ICA connections
□ Use Novell Directory Server credentials

Help:

Use this policy to instruct the client to use the same logon credentials (pass-through authentication) for the Citrix XenApp server as the client computer.

When this policy is enabled, the client can be prevented from using the current user's logon credentials to authenticate to the remote server by clearing the "Enable pass-through authentication" check box.

The client imposes certain restrictions specifying when pass-through authentication can occur (for details, see Citrix eDocs at http://support.citrix.com/proddocs/). If these restrictions are too strict for your environment, select the "Allow pass-through authentication for all ICA connections" check box to bypass the pass-through authentication restrictions.

When run in a Novell Directory Server environment, selecting the "Use Novell Directory Server credentials" check box requests that the client uses the user's NDS credentials.

To configure StoreFront:

When you configure the authentication service on the StoreFront server, select the Domain passthrough 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.

Smart card

Citrix Workspace app for Windows supports the following smart card authentication:

- **Pass-through authentication (Single Sign-on)** - Pass-through authentication captures 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 with smart card credentials can start virtual desktops and applications without needing to reauthenticate.
  - Citrix Workspace app running on non-domain joined devices with smart card credentials must type their credentials again to start an desktop or app.

  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 cannot 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, StoreFront administrator can allow the user 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 available for a single smart card and if multiple smart cards are in use.

- **Client certificate authentication** - Client certificate authentication requires Citrix Gateway and StoreFront configuration.

  - For access to StoreFront through Citrix Gateway, you might have to reauthenticate after removing a smart card.

  - When the Citrix Gateway SSL configuration is set to mandatory client certificate authentication, operation is more secure. However mandatory client certificate authentication is not 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. Deployments supporting double hops are described in the Citrix Virtual Apps and Desktops documentation.
- **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 a 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 only in non-paged memory and not 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 and 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 is not available for smart card users.
- Citrix Workspace app Updater communications with citrix.com and the Merchandising Server are not compatible with smart card authentication on Citrix Gateway.

> **Warning**
>
> Some configuration requires registry edits. Using Registry editor incorrectly might cause problems that can require you to reinstall the operating system. Citrix cannot guarantee that problems resulting from incorrect use of Registry Editor can be solved. Ensure 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.

- Set **SSONCheckEnabled** to false if the single sign-on component is not installed. The key prevents the Citrix Workspace app authentication manager from checking for the single sign-on component, thus allowing Citrix Workspace app to authenticate to StoreFront.

```
HKEY\\_CURRENT\\_USER\Software\Citrix\AuthManager\protocols\
integratedwindows\
```

```
HKEY\\_LOCAL\\_MACHINE\Software\Citrix\AuthManager\protocols\
integratedwindows\
```

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 is logging on to the endpoint with a different method to smart card for Citrix Workspace app for Windows authentication (for example, user name and password), the command line is:

  `/includeSSON LOGON_CREDENTIAL_CAPTURE_ENABLE=No`

This prevents the credentials being captured at logon time and allows Citrix Workspace app to store the PIN when logging on to Citrix Workspace app.

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. Alternatively, 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.
- Key Usage must contain Digital Signature.
- Subject Alternative Name must contain the User Principal Name (UPN).
- Enhanced Key Usage must contain Smart Card log on and Client Authentication, or All Key Usages.
- One of the Certificate Authorities on the certificate's issuer chain must match one of the permitted 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 instead 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\Auth SmartCardPINEntry=CSP.

Smart card support and removal changes

Consider the following when connecting to a XenApp 6.5 PNAgent site:

- Smart card login is supported for PNAgent site logins.
- The smart card removal policy has changed on the PNAgent Site:

A Citrix Virtual Apps session is logged off when the smart card is removed –if the PNAgent site is configured with smart card as the authentication method, the corresponding policy has to be configured on Citrix Workspace app for Windows to enforce the Citrix Virtual Apps session for logoff. Enable roaming for smart card authentication on the XenApp PNAgent site and enable the smart card removal policy, which logs off Citrix Virtual Apps from the Citrix Workspace app session. The user is still logged into the Citrix Workspace app session.

Limitation:

When you log on to the PNAgent site using smart card authentication, the user name is displayed as **Logged On**.

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 secure technologies such as the following:

- Citrix Gateway: For information, see the topics in this section and the Citrix Gateway, and StoreFront documentation.

  > **Note:**
  >
  > Citrix recommends using Citrix Gateway between StoreFront servers and user devices.

- A firewall: Network firewalls can allow or block packets based on the destination address and port. If you are using Citrix Workspace app through a network firewall that maps the server's internal network IP address to an external Internet address (that is, network address translation, or NAT), configure the external address.

- Trusted server.
- For Citrix Virtual Apps or Web Interface deployments only (not applicable to XenDesktop 7) : A SOCKS proxy server or secure proxy server (also known as security proxy server, HTTPS proxy server). You can use proxy servers to limit access to and from your network and to handle connections between Citrix Workspace app and server. Citrix Workspace app supports SOCKS and secure proxy protocols.
- For Citrix Virtual Apps or Web Interface deployments only; not applicable to XenDesktop 7, XenDesktop 7.1, XenDesktop 7.5, or XenApp 7.5: SSL Relay solutions with Transport Layer Security (TLS) protocols.
- For Citrix Virtual Apps and Desktops 7.6, you can enable an SSL connection directly between users and VDAs.

Outbound proxy support

Smart Control allows administrators to define granular policies to configure and enforce user environment attributes for Citrix Virtual Apps and Desktops™ and Citrix DaaS (formerly Citrix Virtual Apps and Desktop service) using Citrix Gateway. For instance, you might want to prohibit users from mapping drives to their remote desktops. This can be achieved using the Smart Control feature on Citrix Gateway.

However, the scenario changes when Citrix Workspace app and Citrix Gateway belong to separate enterprise accounts. In such scenarios, the client domain cannot apply the Smart Control feature because the gateway does not exist on the client domain. Instead, you can leverage thr, Outbound ICA proxy. Outbound ICA proxy lets you use the Smart Control 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. Either a single, static proxy can be configured or the proxy server can be selected at runtime using the outbound proxy plug-in.

You can configure outbound proxies using the following methods:

- Static proxy: Proxy server is configured by providing a proxy hostname and port number.
- Dynamic proxy: A single proxy server can be selected among one or more proxy servers using the proxy plug-in DLL.

You can configure the outbound proxy using the Group Policy Object administrative template and 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 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 hostname 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 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:**

    - 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"
      ```

TLS

This topic applies to Citrix Virtual Apps and Desktops Version 7.6 and later.

To use TLS encryption for all Citrix Workspace app communication with the server, configure the user device, Citrix Workspace app, and, if using Web Interface, the server running the Web Interface. For information about securing StoreFront communications, see Secure section in the StoreFront documentation.

Pre-requisites:

User devices must meet the requirements specified in the System requirements.

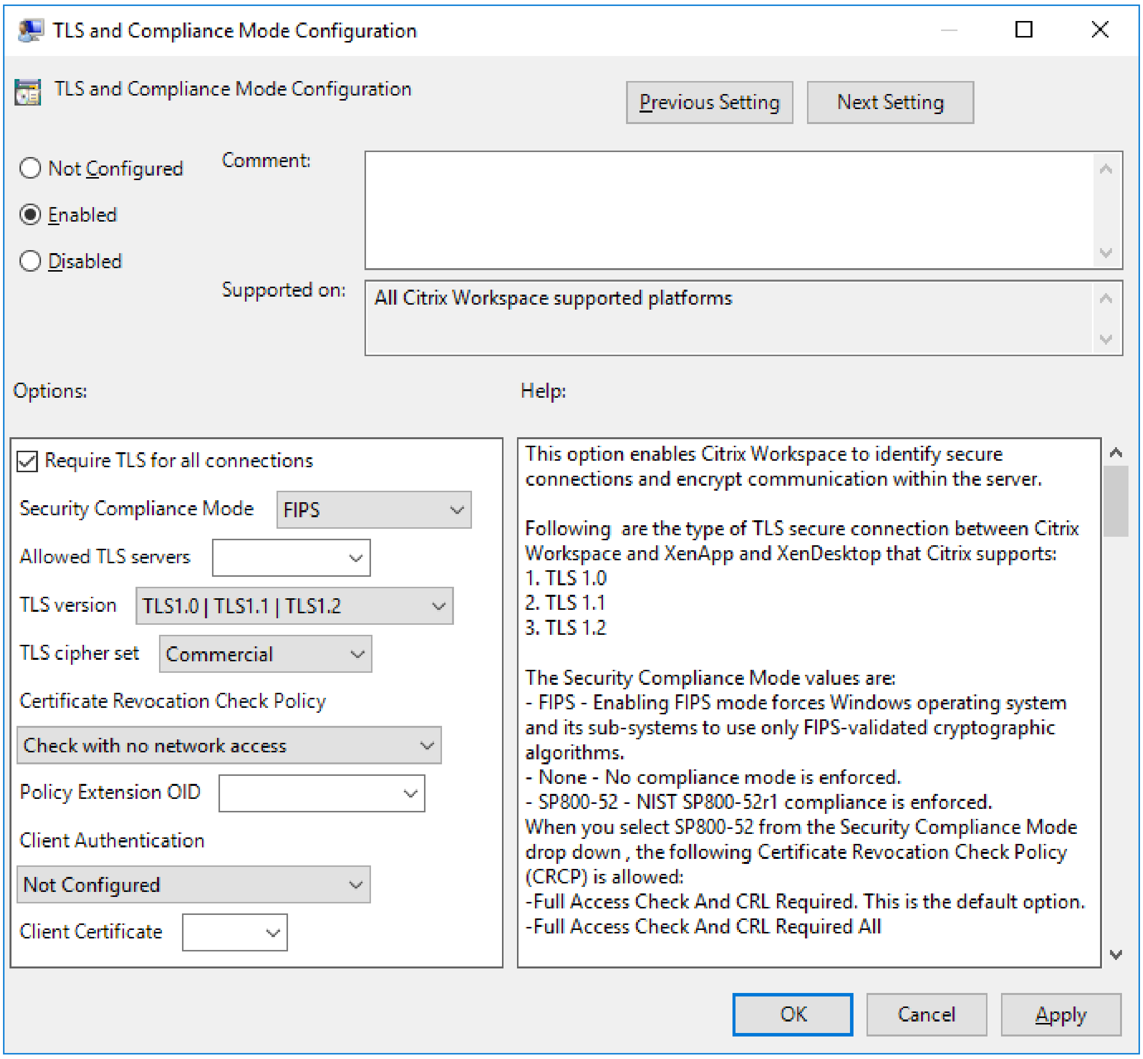
Use this policy to configure the TLS options that ensure the Citrix Workspace app securely identifies the server that it is connecting to, and encrypts all communication with the server.

You can use the options below to:

- Enforce use of TLS: Citrix recommends that all connections over untrusted networks, including the Internet, use TLS.
- Enforce use of FIPS (Federal Information Processing Standards): Approved cryptography and help comply with 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 TLS 1.0, TLS 1.1 and TLS 1.2 protocols between Citrix Workspace app for Windows, and Citrix Virtual Apps and Desktops and Citrix DaaS.
- 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.

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.



TLS and Compliance Mode Configuration

○ Not Configured
● Enabled
○ Disabled

Comment:

Supported on: All Citrix Workspace supported platforms

Options:

☑ Require TLS for all connections

Security Compliance Mode: FIPS

Allowed TLS servers:

TLS version: TLS1.0 | TLS1.1 | TLS1.2

TLS cipher set: Commercial

Certificate Revocation Check Policy: Check with no network access

Policy Extension OID:

Client Authentication: Not Configured

Client Certificate:

Help:

This option enables Citrix Workspace to identify secure connections and encrypt communication within the server.

Following are the type of TLS secure connection between Citrix Workspace and XenApp and XenDesktop that Citrix supports:
1. TLS 1.0
2. TLS 1.1
3. TLS 1.2

The Security Compliance Mode values are:
- FIPS - Enabling FIPS mode forces Windows operating system and its sub-systems to use only FIPS-validated cryptographic algorithms.
- None - No compliance mode is enforced.
- SP800-52 - NIST SP800-52r1 compliance is enforced.
When you select SP800-52 from the Security Compliance Mode drop down , the following Certificate Revocation Check Policy (CRCP) is allowed:
-Full Access Check And CRL Required. This is the default option.
-Full Access Check And CRL Required All

3. Select **Enabled** to enable secure connections and to encrypt communication on the server. Set the following options:

   > **Note:**
   >
   > Citrix recommends TLS for secure connections.

   a) Select **Require TLS for all connections** to force Citrix Workspace app to use TLS for all 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 complies with NIST SP 800-52 recommendations.

> **Note:**
>
> If you select **SP800-52**, FIPS Approved cryptography is automatically used, even if **Enable FIPS** is not selected. You must 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**, you must select either the **Certificate Revocation Check Policy** setting with **Full Access Check**, or **Full access check and CRL required**.

When you select **SP800-52**, Citrix Workspace app verifies that the server certificate complies with 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. You must 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, select the port number. You can ensure that Citrix Workspace app for Windows connects only to a specified server by a comma-separated list. 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 and 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.
- **TLS 1.1 or TLS 1.2** –Use this option to ensure that the ICA 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 the use of specific TLS cipher set, select either Government (GOV), Commercial (COM), or All (ALL). In certain cases of Citrix Gateway configurations, you might need to select **COM**. Citrix Workspace app supports RSA keys of 1024, 2048, and 3072-bit lengths. Root certificates with RSA keys of 4096-bit length are also supported.

> **Note:**
>
> Citrix does not recommend using RSA keys of 1024-bit length

- **Any**: When "Any"is set, the policy is not configured and any of the following cipher suites are allowed:

  a) TLS_RSA_WITH_RC4_128_MD5
  b) TLS_RSA_WITH_RC4_128_SHA
  c) TLS_RSA_WITH_3DES_EDE_CBC_SHA
  d) TLS_RSA_WITH_AES_128_CBC_SHA
  e) TLS_RSA_WITH_AES_256_CBC_SHA
  f) TLS_RSA_WITH_AES_128_GCM_SHA256
  g) TLS_RSA_WITH_AES_256_GCM_SHA384

- **Commercial**: When "Commercial"is set, only the following cipher suites are allowed:

  a) TLS_RSA_WITH_RC4_128_MD5
  b) TLS_RSA_WITH_RC4_128_SHA
  c) TLS_RSA_WITH_AES_128_CBC_SHA
  d) TLS_RSA_WITH_AES_128_GCM_SHA256

- **Government**: When "Government"is set, only the following cipher suites are allowed:

  a) TLS_RSA_WITH_AES_256_CBC_SHA
  b) TLS_RSA_WITH_3DES_EDE_CBC_SHA
  c) TLS_RSA_WITH_AES_128_GCM_SHA256
  d) TLS_RSA_WITH_AES_256_GCM_SHA384

a) From the **Certificate Revocation Check Policy** menu, select any of the following:

- **Check with No Network Access** - Certificate Revocation list check is performed. Only local certificate revocation list stores are used. All distribution points are ignored. Finding the Certificate Revocation List is not mandatory to verify the server certificate that is presented by the target SSL Relay/Citrix Secure Web Gateway server.

- **Full Access Check** - Certificate Revocation List check is performed. Local Certificate Revocation List stores and all distribution points are used. If revocation information for a certificate is found, the connection is rejected. Finding a Certificate Revocation List is not critical for verification of the server certificate presented by the target server.

- **Full Access Check and CRL Required** - Certificate Revocation List check is performed, excluding 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.

- **Full Access Check and CRL Required All** - Certificate Revocation List check is performed, 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 performed.

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 containing that Policy Extension OID.

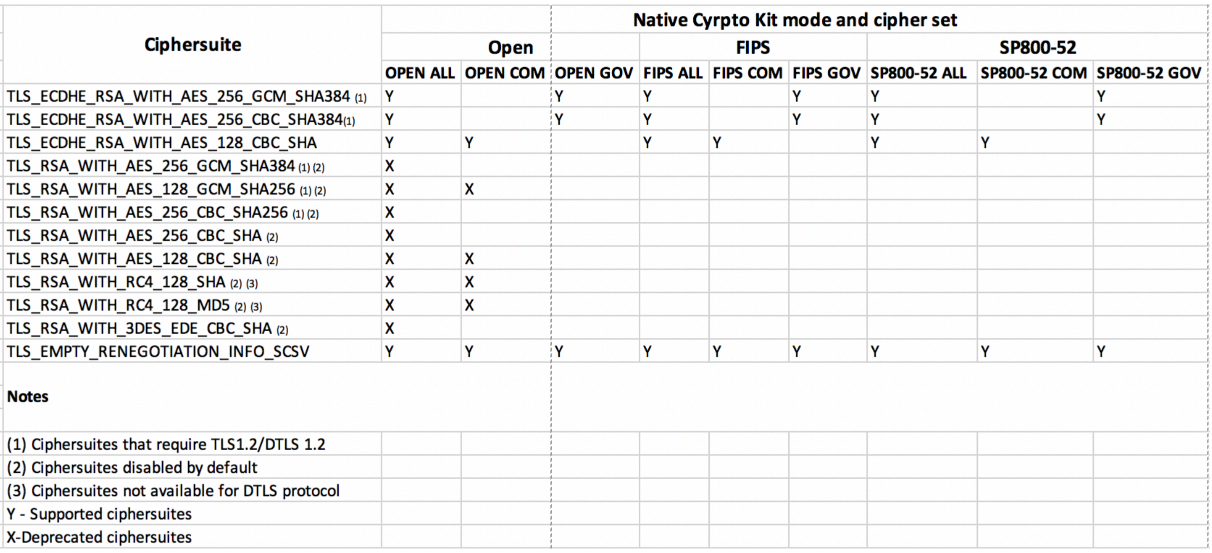
b) From the **Client Authentication** menu, select any of the following:

- **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 is not configured.
- **Use specified certificate** - Use the client certificate as set in the Client Certificate option.

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.

The following table lists the cipher suites in each set:



Ciphersuite	Native Cyrpto Kit mode and cipher set								
	Open			FIPS			SP800-52		
	OPEN ALL	OPEN COM	OPEN GOV	FIPS ALL	FIPS COM	FIPS GOV	SP800-52 ALL	SP800-52 COM	SP800-52 GOV
TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 (1)	Y		Y	Y		Y	Y		Y
TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384(1)	Y		Y	Y		Y	Y		Y
TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA	Y	Y		Y	Y		Y	Y	
TLS_RSA_WITH_AES_256_GCM_SHA384 (1) (2)	X								
TLS_RSA_WITH_AES_128_GCM_SHA256 (1) (2)	X	X							
TLS_RSA_WITH_AES_256_CBC_SHA256 (1) (2)	X								
TLS_RSA_WITH_AES_256_CBC_SHA (2)	X								
TLS_RSA_WITH_AES_128_CBC_SHA (2)	X	X							
TLS_RSA_WITH_RC4_128_SHA (2) (3)	X	X							
TLS_RSA_WITH_RC4_128_MD5 (2) (3)	X	X							
TLS_RSA_WITH_3DES_EDE_CBC_SHA (2)	X								
TLS_EMPTY_RENEGOTIATION_INFO_SCSV	Y	Y	Y	Y	Y	Y	Y	Y	Y
Notes									
(1) Ciphersuites that require TLS1.2/DTLS 1.2									
(2) Ciphersuites disabled by default									
(3) Ciphersuites not available for DTLS protocol									
Y - Supported ciphersuites									
X-Deprecated ciphersuites									

Firewall

Network firewalls can allow or block packets based on the destination address and port. If you are using a firewall in your deployment, Citrix Workspace app for Windows must be able to communicate through the firewall with both the Web server and Citrix server.

Common Citrix Communication Ports

Source	Type	Port	Details
Citrix Workspace app	TCP	80/443	Communication with StoreFront
ICA/HDX	TCP	1494	Access to applications and virtual desktops
ICA/HDX with Session Reliability	TCP	2598	Access to applications and virtual desktops
ICA/HDX over SSL	TCP	443	Access to applications and virtual desktops

For more information on ports, see Knowledge Center article CTX101810.

If the firewall is configured for Network Address Translation (NAT), use the Web Interface to define mappings from internal addresses to external addresses and ports. For example, if your Citrix Virtual Apps and Desktops server is not configured with an alternate address, you can configure the Web Interface to provide an alternate address to Citrix Workspace app. Citrix Workspace app then connects to the server using the external address and port number.

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 or the Web Interface. For information about proxy server configuration, refer to StoreFront or Web Interface documentation.

In communicating with the Web server, Citrix Workspace app uses the proxy server settings that are configured through the **Internet** settings of the default Web browser on the user device. You must configure the **Internet** settings of the default Web browser on the user device accordingly.

Configure the proxy settings using the registry editor to enforce Citrix Workspace app to honor or discard the proxy server during connections.

> **Warning**
>
> Editing the registry incorrectly can cause serious problems that may require you to reinstall your operating system. Citrix cannot guarantee that problems resulting from the incorrect use of Registry Editor can be solved.

1. Navigate to `\HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\Citrix\AuthManager`
2. Set the **ProxyEnabled**(REG_SZ) .
   - True –indicates that Citrix Workspace app honors the proxy server during connections.
   - False - indicates that Citrix Workspace app discards the proxy server during connections.
3. Restart the Citrix Workspace app for the changes to take effect.

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 or not. 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, connected server resides 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

Pre-requisite:

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** > **Classic Administrative Templates(ADM)** > **Citrix Components** > **Citrix Workspace** > **Network Routing** > **Configure trusted server configuration**.
3. Select **Enabled** to force Citrix Workspace app to perform region identification.
4. Select **Enforce trusted server configuration**. This forces the client to perform the identification using a trusted server.

5. From the **Windows internet zone** drop-down, select the client server address. This setting is applicable only to Windows Trusted Site zone.
6. In the **Address** field, set the client server address for trusted site zone other than 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 the launch from untrusted servers. You can configure ICA file signing using the Group policy objects administrative template or StoreFront. ICA file signing is not enabled by default.

For information about enabling ICA file signing for StoreFront, see Enable ICA file signing in StoreFront documentation.

For Web Interface deployment, the Web Interface enables and configures the application or desktop launch to include a signature during the launch using the Citrix ICA file signing service. The service can sign the ICA file using a certificate from the computer's personal certificate store.

Configure ICA file signature

> **Note:**
>
> If the CitrixBase.admx\adml is not 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 whitelist of trusted certificate thumbprints.
    b) Trust Certificates - Click **Show** to remove the existing signing certificate thumbprint from the whitelist. 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 or desktop launch from a trusted server. A security warning appears in case of an invalid signature. You cannot launch the session due to 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, Citrix recommends you choose from the following prioritized 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, such as the Web Interface server certificate.
4. Create a root CA certificate and distribute it to user devices using GPO or manual installation.

Storebrowse

September 13, 2025

Storebrowse is a lightweight command-line utility that is used to interact between the client and the server. It is used to authenticate all the operations within StoreFront and with Citrix Gateway.

For documentation on older version of the Storebrowse utility for Citrix Receiver for Windows, see Storebrowse for Citrix Receiver for Windows documentation.

Using Storebrowse utility, administrators can automate the following day-to-day operations:

- Add a store.
- Enumerate the published Citrix Virtual Apps and Desktops™ and Citrix DaaS (formerly Citrix Virtual Apps and Desktops service) from a configured store.
- Generate an ICA file by selecting any published Citrix Virtual Apps and Desktops and Citrix DaaS manually.
- Generate an ICA® file using the Storebrowse command-line.
- Launch the published application.

The Storebrowse utility is now part of Authmanager component. After installing the Citrix Workspace app, the Storebrowse utility is located in the `AuthManager` installation folder.

You can confirm if the Storebrowse utility is installed along with the `Authmanager` component by checking the registry path in the following ways:

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
On a 64-bit machine	[HKEY_CURRENT_USER\SOFTWARE\WOW6432Node\Citrix\Au

Requirements

Install the Citrix Workspace app Version 1808 for Windows or later for Storebrowse utility to work seamlessly between StoreFront and Citrix Gateway. Citrix Workspace app Version 1809 requires a minimum of 530 MB of free disk space and 2 GB RAM to be installed.

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, Datacenter editions
Windows Server 2012, Standard, and, Datacenter 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

> **Note:**
>
> Storebrowse utility does not accept credentials using command line on an HTTP store.

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**: Users can enter their credentials and are authenticated when they access their stores. Explicit authentication is enabled by default when you create your first store. All user access methods support explicit authentication.
- **Domain Pass-through**: Users authenticate to their domain-joined windows computers and are automatically logged on when they access their stores. To use this option, pass-through authentication must be enabled when Citrix Workspace app is installed on the user devices. For more information on configuring domain pass-through, see Configuring Pass-through authentication.
- **HTTP Basic**: Storebrowse utility requires HTTP Basic authentication to be enabled to communicate with StoreFront servers. This option is disabled by default on StoreFront server. You must enable HTTP Basic authentication method.

Storebrowse utility supports authentication methods in any of the following methods:

- Using the `AuthManager` that is in-built along with Storebrowse utility. Note: You must enable HTTP Basic authentication method on the StoreFront while working with Storebrowse utility. This applies when user provides the credentials using the Storebrowse commands.
- External `Authmanager` that can be included with Citrix Workspace app for Windows.

Citrix Gateway support

With the latest release of Storebrowse utility, you can now add a Citrix Gateway URL. No additional configuration is required in the Storebrowse utility to communicate with Citrix Gateway.

Single sign-on with Citrix Gateway

Additional to the newly added Citrix Gateway support, you can now use single sign-on with it. You can add a new store and enumerate 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 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.

Command usage

The following section provides detailed information about the commands that you can use from Storebrowse utility.

-a, –addstore

Description:

Adds new store. Returns the full URL of the store. If this fails, an error is reported.

> **Note:**
>
> You can add multiple stores using 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

(-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 the available 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 required 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, which can either be the StoreFront server or 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 executing the following command:

```
.\storebrowse -M 0X2000 -E https://myfirstexamplestore.net/Citrix/Second/discovery
```

A typical launch URL looks like below:

```
'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 } -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, which can either be the StoreFront server or Citrix Gateway URL. The ICA file is generated in the `%LocalAppData%\Citrix\Storebrowse\cache` directory.

You can get the display name of the published apps and desktops by executing the command below:

```
.\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 above output is used as input parameter to the launch option.

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:

You can add the store, enumerate the published resources (apps and desktops) and launch the resource with the single command. This option takes the following as parameters - Username, Password, Domain, Friendly name of the resource to be launched and the store URL. However, if the user does not provide the credentials , `AuthManager` prompt is thrown to enter the credentials and then the resource launch will happen.

You can get the name of the resource of published apps and desktops by executing the command below:

```
.\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 above output will be used as 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 required ICA file in the custom path as defined in the –f option for any of the published apps and desktops using the Storebrowse utility.

The launch option requires a folder name along with name of the resource as the input with Store URL, which is either StoreFront server or Citrix Gateway URL.

Command example on StoreFront:

```
.\storebrowse.exe –f “C:\Temp\Launch.ica” –L “Resource_Name” { Store }
```

Command example on Citrix Gateway:

```
.\storebrowse.exe –f “C:\Temp\Launch.ica” –L “Resource_Name” { NSG_URL
 }
```

-t, –traceauthentication

Description:

Generate logs for Storebrowse utility in-built `AuthManager` component. Logs are generated only if Storebrowse utility is using an in-built `AuthManager`. Logs are generated in the `localappdata%\Citrix\Storebrowse\logs` directory.

Note: This option cannot 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 Citrix Virtual Apps and Desktops and Citrix DaaS™ delivered by that domain without having to re-authenticate to each app or desktop. When you add a store using the Storebrowse utility, your credentials are passed through to Citrix Gateway server, along with the virtual apps and desktops enumerated for you, including your Start menu settings. After configuring single sign-on, you can add the store, enumerate the virtual apps and desktops, launch the required resource without having to type your credentials multiple times.

This feature is supported on Citrix Gateway Version 11 and later.

Prerequisites:

For the prerequisites on how to configure Single Sign-On for 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.

> **Note:**
>
> When you upgrade from Citrix Receiver to Citrix Workspace app or fresh install Citrix Workspace app for the first time, you must add the latest template files to the local GPO. For more information on adding template files to the local GPO, see Configuring Group Policy Object administrative template. In case of an upgrade, the existing settings are retained when the latest files are imported.

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:

- HTTP Basic Authentication method must be enabled on the StoreFront server for credential injection operations with Storebrowse utility.

- If you have HTTP store, and when you try connecting to the store using the utility to enumerate 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 which gets triggered when you do not provide credential using the command line.
- Storebrowse utility currently supports only single store configured Citrix Gateway on the StoreFront server.
- Credential Injection in Storebrowse utility works only if 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.

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, which are SSON-enabled (Single Sign-On) and store configured. It does not support PNA sites. Previous versions of Desktop Lock are not supported when you upgrade to Citrix Receiver for Windows 4.2 or later.

Installing Desktop Lock using command-line interface

Prerequisites:

- You must be an administrator on a domain-joined machine.
- Single sign-on must be enabled.
- Store must be configured.

1. Install Citrix Workspace app by running the following command:

```
`CitrixWorkspaceApp.exe /includeSSON /Silent STORE0= “ AppStore;https://testserver.net/Citrix/MyStore/discover;on;Desktop App Store ” `
```

2. Download the `CitrixWorkspaceDesktopLock.msi` available from the Citrix Downloads page.
3. Install the Desktop Lock by running the following command:

   ```
   installationSilent : msiexec /i CitrixWorkspaceDesktopLock.msi /
   qn
   ```

Published desktop is launched automatically after logging in as a user.

System requirements

- Microsoft Visual C++ 2005 Service Pack 1 Redistributable Package. For more information, see the Microsoft Download page.
- Supported on Windows 7 (including Embedded Edition), Windows 7 Thin PC, Windows 8, and Windows 8.1 and Windows 10 (Anniversary update included).
- Connects to StoreFront through native protocols only.
- User devices must be connected to a local area network (LAN) or wide area network (WAN).

Local App Access

> **Important**
>
> Enabling Local App Access might permit local desktop access unless a full lock down 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, 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, with the exception of 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. Log on using a local administrator account.
2. At a command prompt, run the following command (located in the Citrix Workspace app and Plug-ins > Windows > Citrix Workspace app folder on the installation media).

   For example:

```
CitrixWorkspaceApp.exe /includeSSON STORE0="DesktopStore;https://my.
storefront.server/Citrix/MyStore/discovery;on;Desktop Store"
```

For command details, see Install.

1. In the same folder on the installation media, double-click `CitrixWorkspaceDesktopLock.msi`. The Desktop Lock wizard appears. Follow the prompts.
2. When the installation completes, restart the user device. If you have permission to access a desktop and you log on as a domain user, the device appears using Citrix Workspace app Desktop Lock.

To allow administration of the user device after installation, the account used to install `CitrixWorkspaceDeskt`
`.msi` is excluded from the replacement shell. If that account is later deleted, you will not be able to log on 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

Grant access to only one virtual desktop running Citrix Workspace app Desktop Lock per-user.

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.

- Ensure that 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 located 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; no user interaction is required. The virtual desktop is responsible for controlling the USB device and displaying it in the user interface.
    - Enable the USB policy rule.
    - 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) Ensure pass-through authentication with 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 Web Site and use Integrated Windows Authentication.
    g) Ensure the IIS Default Web Site does not 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 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, a consistent smart card removal policy is enforced. 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 as well, regardless of the Windows smart card removal policy set on it. This ensures that the user device is not 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 below.

1. Log on 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.

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 system utility settings menu.
- Win+PrintScrn - Take a screen shot and save to pictures.
- Win+Tab - Open switch list.
- Win+T - Preview open windows in taskbar.

SDK and API

September 7, 2025

Certificate Identity Declaration SDK

The Certificate Identity Declaration (CID) SDK lets developers create a plug-in that lets Citrix Workspace app authenticate to the StoreFront server by using the certificate 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.

Citrix Common Connection Manager SDK

Common Connection Manager (CCM) SDK provides 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 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. This 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 additional 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.
- 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. Using this API, Citrix partners can provide authentication and SSO products that use StoreFront or the Web Interface 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)