Citrix Workspace app for Windows
## Contents

<table>
<thead>
<tr>
<th>Section</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>About this release</td>
<td>3</td>
</tr>
<tr>
<td>Prerequisites to install Citrix Workspace app</td>
<td>16</td>
</tr>
<tr>
<td>Install, Uninstall and Update</td>
<td>22</td>
</tr>
<tr>
<td>Get started</td>
<td>52</td>
</tr>
<tr>
<td>Configure</td>
<td>71</td>
</tr>
<tr>
<td>Authenticate</td>
<td>131</td>
</tr>
<tr>
<td>Secure communications</td>
<td>147</td>
</tr>
<tr>
<td>Storebrowse</td>
<td>159</td>
</tr>
<tr>
<td>Citrix Workspace app Desktop Lock</td>
<td>168</td>
</tr>
<tr>
<td>SDK and API</td>
<td>173</td>
</tr>
<tr>
<td>ICA settings Reference</td>
<td>175</td>
</tr>
</tbody>
</table>
About this release

March 25, 2019

What's new in 1903

Updated framework

Updated the Citrix Secure Browser engine to include the latest security updates, to ensure better security and performance when accessing secure SaaS apps.

What's new in 1902

Enhancement to relative mouse configuration

The relative mouse feature determines how far the mouse has moved since the last frame within a window or screen.
The relative mouse uses the pixel delta between the mouse movements. For example, when you change the direction of the camera using mouse controls, the feature is efficient. Also, apps often hide the mouse cursor because the position of the cursor relative to the screen coordinates is not relevant when manipulating a 3-D object or scene.

So far, the user can enable or disable the feature from the desktop viewer and it is available on a per-session basis. Starting with this release, you can configure the feature both on a per-user and a per-session basis. This gives you more granular control on the availability of the feature.

For more information, see Relative mouse.

Introducing new SDK

The Certificate Identity Declaration (CID) SDK is being introduced with this release. The CID SDK lets developers create a utility using which Citrix Workspace app can authenticate to the StoreFront server by using the certificate installed on the client machine.

For more information, see Certificate Identity Declaration SDK for Citrix Workspace app for Windows documentation.
What’s new in 1812

Updated framework

The Chromium embedded framework on which Citrix Secure Browser is built is updated to Version 70. This results in a better user experience when accessing secure SaaS apps.

What’s new in 1811

Note:

Version 1811 of Citrix Workspace app is packaged with Citrix Virtual Apps and Desktops 7 1811. It is not available separately for download. All features and functionality of Version 1811 are also included in Version 1812.

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, single-monitor desktop sessions, and does not affect any published applications. This configuration applies to all subsequent connections from this client.

Display graphics mode indicator

The Display graphics mode indicator policy has been updated to replace the display lossless indicator policy.

This setting configures the graphics mode indicator to run in the user session. It allows you to see details about the graphics mode in use, including graphics provider, encoder, hardware encoding, image quality, progressive display status, and lossless text.

By default, the Display graphics mode indicator policy is disabled. It replaces the Display lossless indicator policy of earlier releases, which was enabled by default.
DPI matching on Windows 10

DPI matching allows the Windows 10 desktop session to match the DPI of the endpoint when using Citrix Workspace app for Windows.

**Note:**
This setting is disabled by default. DPI matching is enabled whenever the DPI scaling setting is set to **No**. When using VM hosted apps, the DPI is set to 100% by default.

HDX adaptive throughput

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

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

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

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

**Important:**
HDX adaptive throughput changes the way that output buffers are set by moving this mechanism from the client to the VDA. Therefore, adjusting the number of output buffers on the client as described in CTX125027 has no effect.

Client drive mapping performance improvements

Client drive mapping now supports the transfer of data between the host and the client as a stream. This enhancement ensures that the file transfer adapts to the changing network throughput conditions. It also uses any available extra bandwidth to scale up the data transfer rate.

By default, this feature is enabled. These improvements require Citrix Workspace app for Windows 1811 or later.

To disable this feature, set the following registry key and then restart the server:

**Path:** HKEY_LOCAL_MACHINE\System\Currentcontrolset\services\picadm\Parameters
**Name:** DisableFullStreamWrite
**Type:** REG_DWORD
Value:
0x01 - disables
0 or delete - enables

What's new in 1810

Option to choose Citrix Files download location

Citrix Workspace app now lets you select the download location for Citrix Files. Earlier, the download location for Citrix Files, by default, was set to the Downloads folder. Now, the download location is configurable.

You can set the download location using either the Advanced Preferences dialog or the Registry editor.

For information about configuring Citrix Files download location using the Registry editor, see Configuring download location for Citrix Files using the Registry editor.

For information about configuring Citrix Files download location using Advanced Preferences dialog, see Configuring download location using Advanced Preferences in Citrix Workspace app for Windows Help documentation.

Additionally, this release address a number of fixes relating to installation, launch and Citrix Workspace app for Citrix Cloud.

What’s new in 1809

Support for Citrix Ready workspace hub for 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.

Using the Advanced Preferences dialog, you can configure whether you want to launch Citrix Ready workspace hub when Citrix Workspace app is launched.

Note:
- Citrix Casting for Windows supports Citrix Ready workspace hub Version 2.40.3839 and
For more information about Citrix Ready workspace hub in Citrix Workspace app for Windows, see Configuring Citrix Ready workspace hub.

For more information about Citrix Ready workspace hub, see the Citrix Ready workspace hub section in the Citrix Virtual Apps and Desktops documentation.

What’s new in 1808

Secure SaaS with embedded Citrix Secure Browser

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.

For information on how to configure SaaS apps using Access Control Services, see the Access Control documentation.

For more information about SaaS apps with Citrix Workspace app, see Workspace configuration.

Single Sign-on support with Citrix Gateway

Single Sign-on lets you authenticate to a domain and use Citrix Virtual Apps and Desktops delivered by that domain without having to reauthenticate to each app or desktop. When you add a store using the Storebrowse utility, your credentials are passed through to the Citrix Gateway server, along with the apps and desktops enumerated for you, including your Start menu settings. After configuring Single Sign-on, you can add the store, enumerate your apps and desktops, and launch the required resources without having to type your credentials multiple times.

For information about configuring single sign-on with Citrix Gateway, see Configuring single sign-on with Citrix Gateway.
**Beacon test**

With this release, Citrix Workspace app allows you to perform a beacon test using the Beacon checker that is available as part of the [Configuration Checker](#) utility. Beacon test helps to confirm if the beacon (ping.citrix.com) is reachable. This diagnostic test helps to eliminate one of the many possible causes for slow resource enumeration, that is 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.

**Note:**

- The test results are not applicable on Workspace for Web.
- The test results can be saved as reports. The default format for the report is .txt.

**Storebrowse utility for Citrix Workspace app**

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.

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

- Add a store.
- Enumerate the published desktops and applications from a configured store.
- Generate an ICA file manually by selecting any published desktop or application.
- Generate an ICA file using the Storebrowse command-line.
- Launch the published application.

The Storebrowse utility is part of the [Authmanager](#) component. After installing the Citrix Workspace, the Storebrowse utility is located in the AuthManager installation folder. For more information, see the [Storebrowse](#) section.

**Support for PDF printing**

With this release, Citrix Workspace app for Windows supports PDF printing in a session. The Citrix PDF Universal Printer driver allows you to print documents that are launched using hosted applications and desktops running on Citrix Virtual Apps and Desktops.
Citrix Workspace app for Windows

When you select the **Citrix PDF Printer** option from the **Print** dialog, the printer driver converts the file to a PDF and transfers the PDF to the local device. The PDF is then launched using the default PDF viewer for viewing and prints from a locally attached printer.

Citrix recommends Google Chrome browser or Adobe Acrobat Reader for PDF viewing.

You can enable Citrix PDF printing using Citrix Studio on the Delivery Controller.

For information about how to configure PDF printing, see [PDF printing](#).

**Chrome enhancement to browser content redirection**

Browser content redirection now supports the Google Chrome browser in addition to the previously supported Internet Explorer browser. Browser content redirection redirects the contents of a web browser to a client device, and creates a corresponding browser embedded within the Citrix Workspace app. This feature offloads network usage, page processing, and graphics rendering to the endpoint. Doing so improves the user experience when browsing demanding webpages, especially webpages that incorporate HTML5 or WebRTC video.

For more information, see [Browser content redirection](#).

**Better network throughput over high latency connections**

The default number of ICA output buffers that are used to send and receive data has been raised from 44 (64 Kilobytes) to 100 (~145 Kilobytes). This change delivers improved throughput performance even on high latency connections. This enhancement applies to only Citrix Workspace app 1808 for Windows or higher.

For more details, see [CTX125027](#).

**Client drive mapping support for large file transfers**

Client drive mapping now supports transfers of files larger than 4 Gigabytes. The required minimum version for Citrix Workspace app for Windows is 1808.

**Support for Citrix Analytics**

Citrix Workspace app is instrumented to securely transmit logs to Citrix Analytics. The logs are analyzed and stored on Citrix Analytics servers when enabled. For more information about Citrix Analytics, see [Citrix Analytics](#).
Fixed issues

Fixed issues in 1903

This release addresses a number of issues that help to improve overall performance and stability.

Fixed issues in 1902

Installing, Uninstalling, Upgrading

- After you upgrade Citrix Receiver for Windows to Version 4.9 CU4, the registry key that is required for custom virtual channel might not be preserved. [LD0633]

Keyboard

- When the Local IME or the local keyboard layout synchronization feature is enabled if you press the key combination that includes the right Ctrl and right Shift keys, the Shift key might remain stuck in the down position. [LD0585]

Session/Connection

- An authentication issue might occur when there are two stores in different states. One is in the ON state and the other is in the OFF state. [LC9511]
- Start multiple applications within a hosted shared desktop. If you switch between the clients or perform a disconnect or a reconnect operation, this error message might appear:
  Citrix HDX Engine has stopped working
  Exception caused the program to stop working correctly. Please close the program. [LC9772]
- When you attempt to access published desktop applications, the session might disconnect. After the session disconnects, the wfica32.exe process exits unexpectedly. [LC9966]
- The CPU usage of the wfica.32.exe process might be high in a double hop scenario. [LD0386]
- When you run a function that calls a web URL within the Bloomberg terminal published application, the URL might not be redirected to the user device. [LD0484]
- With Application Lingering configured, published applications might fail to reopen an existing file after the session is disconnected. [LD0742]
- Attempts to switch from the front to rear facing camera might fail if the display name of the published desktop contains non-ASCII characters. [LD0732]
System Exceptions

- With the bidirectional content redirection policy enabled, the Redirector.exe process might exit unexpectedly when you attempt to open a webpage on the local web browser. As a result, the bidirectional content redirection does not work, and this error message appears:

  Citrix FTA, URL Redirector stopped working. [LD0420]

- The wfica32.exe process might exit unexpectedly. The issue occurs when the proxy settings are configured and you attempt to start a new session in the Citrix Receiver for Web. [LD0548]

User Interface

- When you select the Reset Receiver option, the Citrix Receiver for Windows might request that you install the .Net Framework 3.5 on Microsoft Windows Version 10. [LD0690]

Fixed issues in 1812

This release addresses a number of issues that help to improve overall performance and stability.

Fixed issues in 1811

Keyboard:

- The mouse clicks might not generate responses on the remote session. This issue can occur when you open the Preferences window from the Desktop Viewer toolbar and configure the MouseTimer setting to any value other than the default value. [LD0260]

Session/Connection:

- Attempts to start an application might fail and this error message appears:

  Unable to launch your application. Contact your help desk and provide them with the following information: Cannot open the Citrix Receiver.

  To enable the fix, the administrator must set the following registry key:

  - Registry key: HKEY_LOCAL_MACHINE\Software\Citrix\ICA Client\Engine
  - Name: EngineTimeout
  - Type: DWORD
  - Value: More than 20 seconds

  To enable the fix, the user must set the following registry key:

  - Registry key: HKEY_LOCAL_MACHINE\Software\Citrix\ICA Client\Engine
  - Name: EngineTimeout
Citrix Workspace app for Windows

- Type: DWORD
- Value: More than 20 seconds, for example, EngineTimeout=20

[LC9771]

- Applications that are started using Citrix Receiver for Windows might be mirrored onto the secondary monitor. [LC9893]
- When using a barcode reader, some of the data might be lost when sending a large amount of data. [LD0243]

Fixed issues in 1810

Session/Connection:

- After you upgrade Citrix Receiver for Windows to Version 4.9.1000, the CDViewer might display a gray screen when you log off. [LC9290]
- A GDI object release issue might cause high CPU usage by the wfica32.exe process. [LC9356]
- After changing the internal beacon point in StoreFront, you might not be able to start applications from Citrix Receiver for Windows until you restart the Citrix Receiver. [LC9442]
- An authentication issue might occur when there are two stores in different states. One is in the ON state and the other is in the OFF state. [LC9511]
- A syntax error might occur in the receiver.admx file that is pushed from Azure Mobile Device Management (MDM) Intune. [LC9992]
- If you do not choose the default program when you configure the File Type Association for .docx for the first time, the following error message might appears:

Windows cannot access the specified device, path, or file. You may not have the appropriate permissions to access the item. [LD0026]

- With this fix, when the minimized window of a seamless application is placed on a desktop rather than the taskbar, the window might appear correctly. [LD0034]

- After you install the Citrix Receiver for Windows 4.12 using the command line with the EnableTracing=false option, the configuration wizard does not start when you right-click Receiver > Open. [LD0156]

- The published instance of certain third-party applications might open as transparent applications when using the NVIDIA graphic cards. [LD0175]

- The local application shortcuts that are created from the Control Panel icon cannot be started with KEYWORDS:Prefer that is configured from Citrix Studio. [LD0288]

- In a user-installed instance of Citrix Workspace app for Windows, launching a published SaaS application might fail. [RFWIN-9329]

As a workaround, perform the following procedure:
1. Launch the Registry editor and navigate to HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\Citrix directory.
2. Create both a folder by name browser and an Expandable String Value registry key by name InstallDir.
3. Set the value of the key to %localAppData%\Citrix\ICAClient.

For more information about this issue, see Knowledge Center article CTX237199.

System Exceptions:

- The Citrix Receiver for Windows might exit unexpectedly and this error message appears: **Citrix HDX Engine has stopped working.**
  
  The issue occurs when there is a trap in the graphics module. [LC9466]

- The **wfica32.exe** process might exit unexpectedly when you log off the system. [LC9892]

- The **wfica32.exe** process might exit unexpectedly when using the command for toggling the generic client IME or the local IME. [LD0038]

Fixed issues in 1809

Logon/Authentication:

- When using Citrix Receiver for Windows to add an account, typing the store URL might result in the following error message: The Authentication Service might not be contacted. The issue occurs when a StoreFront URL begins with the text string citrix.com. [LC9631]

Session/Connection:

- When using Citrix Receiver for Windows 4.10.1, you might not be able to exit from certain published applications. The issue occurs when the confirmation message Are you sure does not appear while you attempt to exit from the applications. [LC9353]

- Attempts to start an application through a secure connection might fail. The issue occurs when the certificate length is long with long subject and log issue names. [LC9853]

- Citrix Receiver for Windows 4.11 might exit intermittently and display this error message: This Application crashed. The issue occurs because of the faulting application, wfica32.exe. [LC9890]

User Interface:

- Non-seamless windows might be resized incorrectly and display scrollbars. [LC9545]

Fixed issues in 1808

Installing, Uninstalling, Upgrading:
• When you attempt to install Citrix Receiver for Windows 4.9.2000 using the silent installation command, the installation process might not complete. [LC9587]

Logon/Authentication:
• After the AuthManSvr.exe process restarts, attempts to log off from Citrix Workspace app for Windows fail. [LC7981]

Session/Connection:
• The Citrix Receiver for Windows 4.7 might fail to redirect the scanners. The issue occurs when the Twain 2.0 device support causes regression with non-Twain 2.0 devices that are running on VDAs. [LC8215]
• After you upgrade Citrix Receiver for Windows from Version 13.x to Version 14.4 using the PSEexec command, attempts to log on to a store might fail. Additionally, Receiver for Windows might become unresponsive during installation or upgrade when using the PSEexec command. With Fix LC9024 installed, the AuthManager components align with other components and install within the ICA client folder. [LC9024]
• With Local App Access enabled, attempts to start a hosted desktop might fail. The desktop appears to have started but remains forever showing a gray screen. [LC9452]
• When you start a Java application (Javaw.exe) with LPT Port Redirection policy enabled, the user session might disconnect. [LC9610]
• Configuration Checker, which validates the single sign-on configuration, might fail to complete the validation process and become stuck verifying the Single Sign-on process. [LC9625]
• When you switch between multiple published applications using the Win+Tab or Alt+Tab keys, the GDI objects might increase on the client until the applications become unresponsive and display black pixels. [LC9655]

User Experience:
• When you use the Japanese Input Method Editor (IME) and input text in an application that is in seamless mode, the text might not be visible. The issue occurs when the font size of the text is small. [LC9882]
  To enable the fix, set the following:
  – Registry key: HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\ICA Client
  – Name: DisableD3DRenderWidthHeightCheck
  – Type: REG_DWORD
  – Value: 1

Known issues

Known issues in 1903

No new issues have been observed in this release.
**Known issues in 1902**

No new issues have been observed in this release.

**Known issues in 1812**

- Image corruption can be observed in sessions running on VDAs with the latest NVIDIA GPUs. Citrix is working on addressing the issue.

**Known issues in 1810**

- Pass-through authentication fails after you upgrade Windows 10 on a computer where Citrix Workspace app is installed. For more information, see Knowledge Center article CTX234973. [TPV-1916]

**Known issues in 1809**

No new issues have been observed in this release.

**Known issues in 1808**

- Exiting the Citrix Workspace app for Windows installation when the splash screen appears might cause conflicts. [RFWIN-9298]

- When you install Citrix Receiver for Windows Version 4.11 on a Windows 10 Operating system (build number 10240), the connection to the VDA might result in a Socket error 10038.

  To fix this issue, upgrade Windows 10 Operating system build number 10240 to Windows 10 Operating system build number 1803.

  For more information, see Knowledge Center article CTX237203.

**Third party notices**

Citrix Workspace app might include third party software licensed under the terms defined in the following document:
Prerequisites to install Citrix Workspace app

March 28, 2019

System requirements and compatibility

Requirements

- This version of Citrix Workspace app requires a minimum of 1 GB RAM.
- .NET Framework minimum requirements
  - Self-Service plug-in requires NET 3.5 Service Pack 1. It allows you to subscribe to and launch the apps and desktops from the Workspace for Windows user interface or command line. For more information, see Using command-line parameters.
  - The .NET 2.0 Service Pack 1.

Compatibility matrix

Citrix Workspace app for Windows is compatible with the following Windows Operating systems and web browsers. It is also compatible with all currently supported versions of Citrix Virtual Apps and Desktops, and Citrix Gateway as listed in the Citrix Product Lifecycle Matrix.

Note:
The Citrix Gateway End Point Analysis Plug-in (EPA) does not support Citrix Workspace app for Windows.

Operating system

<table>
<thead>
<tr>
<th>Operating system</th>
</tr>
</thead>
<tbody>
<tr>
<td>Windows 10 32-bit and 64-bit editions *</td>
</tr>
<tr>
<td>Windows 8.1, 32-bit and 64-bit editions (including Embedded edition)</td>
</tr>
<tr>
<td>Windows 7, 32-bit and 64-bit editions (including Embedded edition)</td>
</tr>
<tr>
<td>Windows Thin PC</td>
</tr>
<tr>
<td>Windows Server 2016</td>
</tr>
<tr>
<td>Windows Server 2012 R2, Standard, and, Datacenter editions</td>
</tr>
<tr>
<td>Windows Server 2008 R2, 64-bit edition</td>
</tr>
<tr>
<td>Windows Server 2019</td>
</tr>
</tbody>
</table>
Citrix Workspace app for Windows

**Operating system**

Windows 10 Enterprise 2016 LTSB 1607

*Supports Windows 10 Version 1607, 1703, 1709, 1803 and 1809.*

**Browser**

- Internet Explorer
- Latest Google Chrome (requires StoreFront)
- Latest Mozilla Firefox
- Microsoft Edge

**Supportability matrix**

<table>
<thead>
<tr>
<th>Operating system supported on touch-enabled devices</th>
<th>Operating system supported on VDA</th>
</tr>
</thead>
<tbody>
<tr>
<td>Windows 10</td>
<td>Windows 10</td>
</tr>
<tr>
<td>Windows 8</td>
<td>Windows 8</td>
</tr>
<tr>
<td>Windows 7</td>
<td>Windows 7</td>
</tr>
<tr>
<td>Windows 7</td>
<td>Windows 2012 R2</td>
</tr>
<tr>
<td>Windows 7</td>
<td>Windows Server 2016</td>
</tr>
<tr>
<td>Windows 7</td>
<td>Windows 2008 R2</td>
</tr>
</tbody>
</table>

**Validating free disk space**

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

<table>
<thead>
<tr>
<th>Installation type</th>
<th>Required disk space</th>
</tr>
</thead>
<tbody>
<tr>
<td>Fresh installation</td>
<td>572 MB</td>
</tr>
<tr>
<td>Upgrade</td>
<td>350 MB</td>
</tr>
</tbody>
</table>
Citrix Workspace app for Windows

Citrix Workspace app performs a check to verify whether there is enough available disk space to complete the installation. The verification is performed both during a fresh installation and an upgrade. During a fresh installation, the installation stops when there is insufficient disk space and the following dialog appears.

When you are upgrading Citrix Workspace app, the installation ends when there is insufficient disk space and the following dialog appears.

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

Connections, Certificates, and Authentication

Connections

- HTTP store
- HTTPS store
Citrix Workspace app for Windows

- Citrix Gateway 10.5 and later
- Web Interface 5.4

Certificates

- 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.

Installing 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

<table>
<thead>
<tr>
<th></th>
<th>Workspace for Web using browsers</th>
<th>StoreFront Services site (native)</th>
<th>StoreFront, Citrix Virtual Apps and Desktops (native)</th>
<th>Citrix Gateway to Workspace for Web (browser)</th>
<th>Citrix Gateway to StoreFront Services site (native)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Anonymous</td>
<td>Yes</td>
<td>Yes</td>
<td></td>
<td>Yes*</td>
<td>Yes*</td>
</tr>
<tr>
<td>Domain</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes*</td>
<td>Yes*</td>
</tr>
<tr>
<td>Domain pass-through</td>
<td>Yes</td>
<td>Yes</td>
<td></td>
<td>Yes</td>
<td></td>
</tr>
<tr>
<td>Security token</td>
<td></td>
<td></td>
<td></td>
<td>Yes*</td>
<td>Yes*</td>
</tr>
<tr>
<td>Two-factor authentication (domain with security token)</td>
<td></td>
<td></td>
<td></td>
<td>Yes*</td>
<td>Yes*</td>
</tr>
<tr>
<td>SMS</td>
<td></td>
<td></td>
<td></td>
<td>Yes*</td>
<td>Yes*</td>
</tr>
<tr>
<td>Smart card</td>
<td>Yes</td>
<td>Yes</td>
<td></td>
<td>Yes</td>
<td></td>
</tr>
<tr>
<td>User certificate</td>
<td></td>
<td></td>
<td></td>
<td>Yes (Citrix Gateway plug-in)</td>
<td>Yes (Citrix Gateway plug-in)</td>
</tr>
</tbody>
</table>

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

Note:
Citrix Workspace app for Windows

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):

<table>
<thead>
<tr>
<th>Authentication Method</th>
<th>Web Interface (browsers)</th>
<th>Web Interface Citrix Gateway Site</th>
<th>Citrix Gateway to Web Interface (browser)</th>
<th>Citrix Gateway to Web Interface Citrix Gateway Site</th>
</tr>
</thead>
<tbody>
<tr>
<td>Anonymous</td>
<td>Yes</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Domain</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes*</td>
<td></td>
</tr>
<tr>
<td>Domain pass-through</td>
<td>Yes</td>
<td>Yes</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Security token</td>
<td></td>
<td></td>
<td>Yes*</td>
<td></td>
</tr>
<tr>
<td>Two-factor authentication (domain with security token)</td>
<td></td>
<td></td>
<td>Yes*</td>
<td></td>
</tr>
<tr>
<td>SMS</td>
<td></td>
<td></td>
<td></td>
<td>Yes*</td>
</tr>
<tr>
<td>Smart card</td>
<td>Yes</td>
<td>Yes</td>
<td></td>
<td></td>
</tr>
<tr>
<td>User certificate</td>
<td></td>
<td></td>
<td></td>
<td>Yes (Citrix Gateway plug-in)</td>
</tr>
</tbody>
</table>

* 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 and Manage topics in the StoreFront documentation.

**Certificate revocation list**

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

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

If you are making this change on your local computer, exit Citrix Workspace app. Ensure all the Citrix Workspace components, including the Connection Center, are closed.

For information about configuring TLS, see Configure and enable TLS

Install, Uninstall and Update

March 25, 2019

You can install the Citrix Workspace app using any of the following methods:

- Download the CitrixWorkspaceApp.exe installation package from the Citrix Workspace app Download page or from your company’s download page (if available). The package can be installed by:
  - Running an interactive Windows-based installation wizard. Or
  - Typing the installer filename, installation commands and installation properties using the command line interface. For information about installing Citrix Workspace app using command line interface, see Using command-line parameters.
- 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 startup scripts.
- Deploy Citrix Workspace app for Windows using Workspace for Web to ensure that the users have installed the 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.

Prerequisites:

- Verify that the system meets the system requirements as prescribed.

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.

Installation with administrator and non-administrator privileges:

The following differences exist between installations of Citrix Workspace app for Windows performed by an administrator and those performed by a user (non-administrator).
Citrix Workspace app for Windows

<table>
<thead>
<tr>
<th>Installation folder</th>
<th>Installation type</th>
</tr>
</thead>
<tbody>
<tr>
<td>Administrator</td>
<td>C:\Program Files (x86)\Citrix\ICA Client</td>
</tr>
<tr>
<td>User</td>
<td>%USERPROFILE%\AppData\Local\Citrix\ICA Client</td>
</tr>
</tbody>
</table>

**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 Windows before installing Citrix Workspace app for Windows as an administrator.

**Install manually**

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. For command line installation parameters, see Using command-line parameters. Citrix Workspace app can be installed by a user as well as an administrator. Administrator privileges are required only when using pass-through authentication with Citrix Workspace app for Windows.

**To install Citrix Workspace app using a Windows-based installer:**

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

For more information about system requirements, see System requirements.
Citrix Workspace app for Windows

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:

1. Common parameters
2. Install parameters
3. HDX features parameters
4. Preferences and user interface parameters
5. Authentication parameters

**Common parameters**

- `/?` or `/help` - Lists all the installation commands and properties.
- `/silent` - Disables installation dialogs and prompts during installation.
- `/noreboot` - Suppresses the prompts to reboot dialog during installation. When you suppress the reboot prompt, the USB devices that are in a suspended state are not recognised by Workspace app until after the user device is restarted.
- `/includeSSON` - Requires you to install as an administrator. Indicates that the Citrix Workspace app is installed with the single sign-on component. See Domain pass-through authentication for more information.
- `/rcu` - Indicates that Citrix Workspace app will be installed/upgraded by uninstalling existing version of the software. This also cleans up older settings.

**Install parameters**

`/AutoUpdateCheck`

**Description:**

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 updates are available. Check for updates manually. Example, `CitrixWorkspaceApp.exe /AutoUpdateCheck=manual`.
Citrix Workspace app for Windows


/AutoUpdateStream

Description:
Indicates the release track of Citrix Workspace app. See Lifecycle Milestones for more information.
- LTSR – Indicates that the release is a Long Term Service Release. Example, `CitrixWorkspaceApp.exe /AutoUpdateStream=LTSR`.
- Current – Indicates that the release is the latest version of Citrix Workspace app. Example, `CitrixWorkspaceApp.exe /AutoUpdateStream=Current`.

/DeferUpdateCount

Description:
Indicates the number of times that you can defer the update notification when an update is available. See Citrix Workspace Updates for more information.
- -1 (default) - Allows deferring notification any number of times. Example, `CitrixWorkspaceApp.exe /DeferUpdateCount=-1`.
- 0 – Indicates that you will receive one notification (only) for every available update. The Remind me later option is disabled. Example, `CitrixWorkspaceApp.exe /DeferUpdateCount=0`.
- Any other number ‘n’ – Allows deferring the update notification ‘n’ number of times. The Remind me later option is displayed in the ‘n’ count. Example, `CitrixWorkspaceApp.exe /DeferUpdateCount=<n>`.

/AURolloutPriority

Description:
Indicates the period when you can stage the rollout.
- Auto (default) - Updates are rolled out during the delivery period as configured by the administrator. Example, `CitrixWorkspaceApp.exe /AURolloutPriority=Auto`.
- Fast – Updates are rolled out at the beginning of the delivery period. Example, `CitrixWorkspaceApp.exe /AURolloutPriority=Fast`.
- Medium- Updates are rolled out at the mid-delivery period. Example, `CitrixWorkspaceApp.exe /AURolloutPriority=Medium`.
- Slow – Updates are rolled out at the end of the delivery period. Example, `CitrixWorkspaceApp.exe /AURolloutPriority=Slow`.

© 1999-2019 Citrix Systems, Inc. All rights reserved.
**INSTALLDIR**

**Description:**

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

**ADDLOCAL**

**Description:**

Installs one or more of the specified components. Example, `CitrixWorkspaceApp.exe ADDLOCAL=ReceiverInside,ICA_Client,AM,SELSERVICE,DesktopViewer,Flash,Vd3d,WebHelper,BrowserEngine,WorkspaceHub`.

**HDX features parameters**

**ALLOW_BIDIRCONTENTREDIRECTION**

**Description:**

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

**FORCE_LAA**

**Description:**

Indicates that Citrix Workspace app is installed with the client-end local app access component. See the [Local App Access](#) section in Citrix Virtual Apps and Desktops documentation for more information.

- 2-0 (default) - Indicates that local app access component is not installed. Example, `CitrixWorkspaceApp.exe FORCE_LAA =2`.
- 3-1 - Indicates that the client-end local app access component is installed. Example, `CitrixWorkspaceApp.exe FORCE_LAA =1`.
LEGACYFTAICONS

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

- False (default)- Indicates that the 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 the application icons are not displayed for documents or files that have file type associations with subscribed applications. Example, `CitrixWorkspaceApp.exe LEGACYFTAICONS=True`.

ALLOW_CLIENTHOSTEDAPPSURL

Description:
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 the user device. Example, `CitrixWorkspaceApp.exe ALLOW_CLIENTHOSTEDAPPSURL=0`.
- 1- Enables the URL redirection feature on the user devices. Example, `CitrixWorkspaceApp.exe ALLOW_CLIENTHOSTEDAPPSURL=1`.

Preference and user interface parameters

ALLOWSAVEPWD

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

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

DESC TOPDIR

Description:
Specifies the directory for shortcuts on Desktop.

- `<Directory Name>` - By default, shortcuts appear inside the `\Desktop` folder. You can specify the relative path of the shortcuts. For example, to place shortcuts under Start > All Programs > Workspace, specify `STARTMENUDIR=Workspace`. Example, `CitrixWorkspaceApp.exe DESKTOPDIR=\Office`.

SELF SERVICEMODE

Description:
Controls access to the self-service Workspace app user interface. See Session Management in Fast Connect 3 Credential Insertion API documentation.

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

ENABLEPRELAUNCH

Description:
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

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

- 0 (default) – Displays both Shortcuts and Reconnect options in the Advanced Preferences sheet. Example, `CitrixWorkspaceApp.exe DisableSetting=0`.

© 1999-2019 Citrix Systems, Inc. All rights reserved.
Citrix Workspace app for Windows

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

**EnableCEIP**

**Description:**
Indicates your participation in the Customer Experience Improvement Program. See [CEIP](#) for more information.

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

**EnableTracing**

**Description:**
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**

**Description:**
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%`.

**STARTMENUDIR**

**Description:**
Specifies the directory for the shortcuts in the Start menu.
Citrix Workspace app for Windows

- **<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**. Example, CitrixWorkspaceApp.exe STARTMENUDIR=\Office.

**ENABLE_DYNAMIC_CLIENT_NAME**

**Description:**
Allows 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**

**Description:**
Enables single sign on when the 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**

**Description:**
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.
Citrix Workspace app for Windows

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

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

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

**Values:**

- **x** - Integers 0 through 9 used to identify a store.
- **storename** - Name of the store. This value must match the name configured on the StoreFront server.
- **servername.domain** - The fully qualified domain name of the server hosting the store.
- **IISLocation** - the path to the store within IIS. The store URL must match the URL in the StoreFront 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** - An optional description of the store, such as **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.

**Upgrading from an unsupported Citrix Workspace app version**

**Note:**

When you upgrade Citrix Receiver for Windows Version 13.x Enterprise or 12.x to Citrix Receiver for Windows Version 4.4 or later using the graphical user interface, the installer runs the Receiver cleanup utility by default.

However, when you upgrade from the command-line, the utility does not run by default. To upgrade from the command-line, run the following command:

`CitrixWorkspaceApp.exe /rcu /silent`

When you upgrade Citrix Receiver for Windows from 13.x (non-Enterprise) or 4.1 to Version 4.2 or later, the `/rcu` switch is unnecessary and ignored.
Citrix Workspace app for Windows

Troubleshooting the installation

If there is a problem with the installation, search in the user’s %TEMP%/CTXWorkspaceInstallLogs directory for the logs with the prefix CtxInstall- or TrolleyExpress-. For example,

CtxInstall-ICAWebWrapper-20141114-134516.log
TrolleyExpress-20090807-123456.log

Examples of a command line installation

To specify the Citrix Gateway store URL:

1 CitrixWorkspaceApp.exe HRStore;https://ag.mycompany.com#Storename;On;Store

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

Note:
- The Citrix Gateway store URL configured using this method does not support the PNA Services Sites that are using Citrix Gateway.

To install all components silently and specify two application stores:

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

To specify single sign-on (pass-through authentication) and add a store that points to a XenApp Services URL:

1 CitrixWorkspaceApp.exe /INCLUDESSON
2 /STORE0="PNAgent;https://testserver.net/Citrix/PNAgent/config.xml;on;MyPNAgent Site"

Using Active Directory and sample startup 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 Microsoft documentation.
To use the startup 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 sample 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.

Per-computer configuration using startup scripts

Citrix includes sample per-computer startup scripts to install and uninstall Citrix Workspace app. The scripts are located on the Citrix Workspace app for Windows Download page.

- `CheckAndDeployWorkspacePerMachineStartupScript.bat`
- `CheckAndRemoveWorkspacePerMachineStartupScript.bat`

To add the startup scripts:

1. Open the Group Policy Management Console.
2. Select **Computer Configuration > Policies > Windows Settings > Scripts (Startup/Shutdown)**.
3. In the right pane of the Group Policy Management Console, select **Startup**.
4. In the Properties menu, click **Show Files**, copy the appropriate script to the folder displayed, and close the dialog.
5. In the Properties menu, click **Add** and select **Browse** to 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.

Per-user configuration using startup scripts

Citrix recommends using per-user startup scripts. For Windows per-user deployments, the following two Citrix Workspace app for Windows per-user scripts are included on the Citrix Virtual Apps and Desktops media in the Citrix Workspace for Windows and Plug-ins\Windows\Workspace\Startup\Logon\Scripts folder.

- CheckAndDeployWorkspacePerUserLogonScript.bat
- CheckAndRemoveWorkspacePerUserLogonScript.bat

To add the startup scripts:

1. Open the Group Policy Management Console.
3. In the right-hand pane of the Group Policy Management Console, select Logon.
4. In the Logon Properties menu, click Show Files, copy the appropriate script to the folder displayed, and then close the window.
5. In the Logon Properties menu, click Add and use Browse to find and add the newly created script.

To deploy Citrix Workspace app for Windows:

1. Move the users designated to receive this deployment to the OU you created.
2. Reboot the user device and log on as the specified user.
3. Verify that Program and Features (Add or Remove Programs in previous OS versions) contain the newly installed package.

To remove Citrix Workspace app for Windows:

1. Move the users designated for the removal to the OU you created.
2. Reboot the user device and log on as the specified user.
3. Verify that Program and Features (Add or Remove Programs in previous OS versions) removed the previously installed package.
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 the 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.
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:
- **Version**

Operator:
- **Greater than or equal to**

Value:
- Type **4.3.0.65534**

**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
Citrix Workspace app for Windows

- **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).
Citrix Workspace app for Windows

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.

**Uninstall**

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.

**Uninstall 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
```

The registry keys created by receiver.adm/receiver.adml or receiver.admx remain in the Software\Policies\Citrix\ICA Client directory under HKEY_LOCAL_MACHINE and HKEY_LOCAL_USER after uninstallation.

When you reinstall Citrix Workspace app for Windows, these policies might be enforced, possibly causing unexpected behavior. To remove the customizations, delete them manually.

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

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

**Upgrade**

**Manual Upgrade to Citrix Workspace app for Windows**

For deployments with StoreFront:
• Best practice for BYOD (Bring Your Own Device) users is to configure the latest versions of Citrix Gateway and StoreFront as described in the documentation for those products on the Product Documentation site. Attach the provisioning file created by StoreFront to an email and inform users how to upgrade and to open the provisioning file after installing Citrix Workspace app for Windows.

• As an alternative to providing a provisioning file, inform users to enter the Citrix Gateway URL. Or, if you configured email-based account discovery as described in the StoreFront documentation, inform users to enter their email address.

• Another method is to configure Workspace for Web site as described in the StoreFront documentation and complete the configuration described in Using Workspace for Web. Inform users how to upgrade Citrix Workspace app for Windows, access the Workspace for Web site, and download the provisioning file from Workspace for Web (click the user name and click Activate).

Considerations when upgrading:

For information about considerations before upgrading Citrix Workspace app for Windows, see the Knowledge Center article CTX135933.

Upgrading Citrix Workspace app

To upgrade to the latest Citrix Workspace app, do any of the following steps:

• Download the Citrix Workspace app from the Citrix download page.
• Upgrade your Citrix Workspace app using your app store.
• Auto update to Citrix Workspace app from Citrix Receiver using Citrix Workspace Updates.

Citrix Workspace Updates

When you configure Citrix Workspace Updates from Citrix Workspace app, follow the methods below in the order of priority:

1. Group Policy Object administrative (GPO) template
2. Command line interface
3. Advanced Preferences (per-user)

Note:

• When you upgrade Citrix Workspace app using Citrix Workspace Updates, the log in window does not appear.
• 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 versions of Citrix Workspace app.

Limitations:
1. If you have configured an SSL intercepting outbound proxy, you must add an exception to the Workspace auto-update Signature service https://citrixupdates.cloud.com/ and the download location https://downloadplugins.citrix.com/.
2. Your system must have access to the internet.
3. Workspace for Web users cannot download the StoreFront policy automatically.
4. By default, Citrix Workspace Updates is disabled on the VDA. This includes RDS multi-user server machines, VDI and RemotePC machines.
5. Citrix Workspace Updates is disabled on machines where Desktop Lock is installed.

**Configure Citrix Workspace Updates using the Group Policy Object administrative template**

1. Open the Citrix Workspace app Group Policy Object administrative template by running gpedit.msc.
2. Under the Computer Configuration node, go to Administrative Templates > Citrix Components > Citrix Workspace > Workspace Updates.
3. Select the Set the Delay in Checking for Update policy. This policy allows you to stage the rollout for a period.
4. Select **Enabled**, and from the **Delay Group** drop-down, select one of the following options:

   - **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.

5. Click **Apply** and **OK** to save the Policy.

6. In the Workspace Updates Templates section, select the **Citrix Workspace Updates** policy.
When you select Disabled, you are not notified of the available updates. This also hides the Workspace Updates option from the Advanced Preferences sheet.

7. Select Enabled and set the values as required:

- From the Enable Citrix Workspace Update Policy drop-down, select one of the following options:
  - Auto - You are notified when an update is available (default).
  - Manual - You are not notified when updates are available. Check for updates manually.
- Select LTSR ONLY to get updates for LTSR only.
- From the Auto-Update-DeferUpdate-Count drop-down, select a value between -1 and 30, where
  - -1 indicates that you can defer the notifications any number of times (default value=-1).
Citrix Workspace app for Windows

- 0 indicates that the **Remind me later** option is not displayed.
- Any other number indicates that the **Remind me later** option is displayed on that count. For example, if you set the value to 10, the **Remind me later** option is displayed 10 times.

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

---

**Configure Citrix Workspace Updates using the command line interface**

**While installing Citrix Workspace app for Windows:**

To configure Citrix Workspace Updates settings as an administrator using command-line settings during Citrix Workspace app for Windows installation:

- /AutoUpdateCheck= auto/manual/disabled
- /AutoUpdateStream= LTSR/Current. Where, LTSR refers to Long Term Service Release and Current refers to the current release.
- /DeferUpdateCount= any value between -1 and 30
- /AURolloutPriority= auto/fast/medium/slow

For example - **CitrixWorkspaceApp.exe /AutoUpdateCheck=auto /AutoUpdateStream=Current /DeferUpdateCount=-1 /AURolloutPriority=fast**

- To configure Citrix Workspace Updates settings as a user using command-line settings during Citrix Workspace for Windows installation
  /AutoUpdateCheck=auto/manual

For example: **CitrixWorkspaceApp.exe /AutoUpdateCheck=auto**

Editing Citrix Workspace Updates settings using the Group Policy Object administrative template overrides the settings applied during Citrix Workspace app installation for all users.

**After Citrix Workspace app for Windows installation:**

Citrix Workspace Updates can be configured after installing Citrix Workspace app for Windows.

**To use the command line:**

Open Windows Command Prompt and change the directory to where **CitrixWorkspaceUpdater.exe** is located. Typically, CitrixWorkspaceUpdater.exe is located at **CitrixWorkspaceInstallLocation\Citrix\IcaClient\Workspace**.

You can also set the Citrix Workspace Updates command-line policy using this binary.

For example, Administrators can use all the four options:

- **CitrixWorkspaceUpdater.exe /AutoUpdateCheck=auto /AutoUpdateStream=Current/DeferUpdateCount=-1 /AURolloutPriority=fast**
Configure Citrix Workspace Updates using the graphical user interface

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 Hiding the Advanced Preferences sheet.

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

1. Right-click Citrix Workspace app icon from the notification area.
2. Select Advanced Preferences and click Workspace Updates.

![Image of Do you want to be notified when updates are available?]

3. Select one of the following options:
   - Yes, notify me
   - No, don't notify me
   - Use administrator specified settings
4. Click Save.

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:
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="true"/>
          </properties>
      </annotatedServiceRecord>
    </annotatedServices>
  </account>
</account>
```
auto-update-Check

This attribute indicates that Citrix Workspace app detects when an update is available.

Valid values:

• Auto – You are notified when an update is available (default).
• Manual – You are not notified when updates are available. Check for updates manually.
• Disabled – The Citrix Workspace Updates is hidden and you will not be notified when an update is available.

**auto-update-LTSR-Only**

This attribute indicates that Citrix Workspace app must accept updates only for LTSR.

**Valid values:**

• True – Citrix Workspace Updates checks only for LTSR updates of Citrix Workspace app for Windows
• False – Citrix Workspace Updates checks for non-LTSR updates of Citrix Workspace app for Windows as well.

**auto-update-DeferUpdate-Count**

This attribute indicates the number of counts you can defer the notifications. The **Remind me later** option is displayed in the count of the set value.

**Valid values:**

• -1 – indicates that you can defer the notifications any number of times (default value=-1).
• 0 – indicates that the Remind me later option is not displayed.
• Any other number – indicates that the Remind me later option is displayed in that count. For example, if you set the value to 10, the Remind me later option is displayed 10 times.

**auto-update-Rollout-Priority**

This attribute indicates the period that you can set for the rollout.

**Valid values:**

• 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.

**Get started**

February 27, 2019

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 the System requirements section.

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

- Group Policy Object administrative template
- StoreFront
- User accounts
- Client drive mapping
- DNS 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 the 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.

<table>
<thead>
<tr>
<th>File type</th>
<th>File location</th>
</tr>
</thead>
<tbody>
<tr>
<td>receiver.adm</td>
<td>&lt;Installation Directory&gt;\ICA Client\Configuration</td>
</tr>
<tr>
<td>receiver.admx</td>
<td>&lt;Installation Directory&gt;\ICA Client\Configuration</td>
</tr>
<tr>
<td>receiver.adml</td>
<td>&lt;Installation Directory&gt;\ICA Client\Configuration[MUIculture]</td>
</tr>
<tr>
<td>CitrixBase.admx</td>
<td>&lt;Installation Directory&gt;\ICA Client\Configuration</td>
</tr>
<tr>
<td>CitrixBase.adml</td>
<td>&lt;Installation Directory&gt;\ICA Client\Configuration[MUIculture]</td>
</tr>
</tbody>
</table>

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 Templates 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 for Windows

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:

<table>
<thead>
<tr>
<th>File type</th>
<th>Copy from</th>
<th>Copy to</th>
</tr>
</thead>
<tbody>
<tr>
<td>receiver.admx</td>
<td>Installation Directory\ICA\Client\Configuration\receiver.admx</td>
<td>%systemroot%\policyDefinitions</td>
</tr>
<tr>
<td>CitrixBase.admx</td>
<td>Installation Directory\ICA\Client\Configuration\CitrixBase.admx</td>
<td>%systemroot%\policyDefinitions</td>
</tr>
<tr>
<td>receiver.adml</td>
<td>Installation Directory\ICA\Client\Configuration[MUIculture]\receiver.adml</td>
<td>%systemroot%\policyDefinitions[\MUIculture]</td>
</tr>
<tr>
<td>CitrixBase.adml</td>
<td>Installation Directory\ICA\Client\Configuration[MUIculture]\CitrixBase.adml</td>
<td>%systemroot%\policyDefinitions[\MUIculture]\CitrixBase.adml</td>
</tr>
</tbody>
</table>

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, 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 Configure and install Workspace for Windows 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.
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: https://dtls.blrwinrx.com #Store name.On; Store for HR staff
Where #Store name is the name of store behind Citrix Gateway; dtls.blrwinrx.com is the Citrix Gateway URL.

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.
- Any change in Citrix Gateway URL requires the Citrix Workspace app to be reset for the changes to take effect.
- 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\_CURRENT\_USER\SOFTWARE\Wow6432Node\Citrix\Dazzle (64-bit)

HKEY\_CURRENT\_USER\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\_CURRENT\_USER\SOFTWARE\Wow6432Node\Citrix\Dazzle (64-bit)

HKEY\_CURRENT\_USER\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\ICA\CLIENT\Engine\. The REG_DWORD value can be set to 4 if you want the status indicator to disappear sooner.

Customizing location for application shortcut using command line

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:
<table>
<thead>
<tr>
<th>Registry key</th>
<th>Value</th>
<th>Key path</th>
</tr>
</thead>
<tbody>
<tr>
<td>WSCSupported</td>
<td>True</td>
<td>- HKEY_CURRENT_USER \ SOFTWARE \Citrix\Dazzle</td>
</tr>
<tr>
<td></td>
<td></td>
<td>- HKEY_CURRENT_USER \ SOFTWARE \Citrix\Receiver \SR\Store\ + primaryStoreID + \Properties</td>
</tr>
<tr>
<td></td>
<td></td>
<td>- HKEY_LOCAL_MACHINE \SOFTWARE\Policies\Citrix \Dazzle</td>
</tr>
<tr>
<td></td>
<td></td>
<td>- HKEY_LOCAL_MACHINE \SOFTWARE\Citrix\Dazzle</td>
</tr>
<tr>
<td>WSCReconnectAll</td>
<td>True</td>
<td>- HKEY_CURRENT_USER \ SOFTWARE \Citrix\Dazzle</td>
</tr>
<tr>
<td></td>
<td></td>
<td>- HKEY_CURRENT_USER \ SOFTWARE \Citrix\Receiver \SR\Store\ + primaryStoreID + \Properties</td>
</tr>
<tr>
<td></td>
<td></td>
<td>- HKEY_LOCAL_MACHINE \SOFTWARE\Policies\Citrix \Dazzle</td>
</tr>
<tr>
<td></td>
<td></td>
<td>- HKEY_LOCAL_MACHINE \SOFTWARE\Citrix\Dazzle</td>
</tr>
<tr>
<td>WSCReconnectMode</td>
<td>3</td>
<td>- HKEY_CURRENT_USER \ SOFTWARE \Citrix\Dazzle</td>
</tr>
<tr>
<td></td>
<td></td>
<td>- HKEY_CURRENT_USER \ SOFTWARE \Citrix\Receiver \SR\Store\ + primaryStoreID + \Properties</td>
</tr>
<tr>
<td></td>
<td></td>
<td>- HKLM\SOFTWARE\Policies\Citrix \Dazzle</td>
</tr>
<tr>
<td></td>
<td></td>
<td>- HKLM\SOFTWARE\Citrix\Dazzle</td>
</tr>
<tr>
<td>WSCReconnectModeUser</td>
<td>Registry is not created during installation</td>
<td>- HKEY_CURRENT_USER \ SOFTWARE \Citrix\Dazzle</td>
</tr>
<tr>
<td></td>
<td></td>
<td>- HKEY_CURRENT_USER \ SOFTWARE \Citrix\Receiver \SR\Store\ + primaryStoreID + \Properties</td>
</tr>
<tr>
<td></td>
<td></td>
<td>- HKEY_LOCAL_MACHINE \SOFTWARE\Policies\Citrix \Dazzle</td>
</tr>
<tr>
<td></td>
<td></td>
<td>- HKEY_LOCAL_MACHINE \SOFTWARE\Citrix\Dazzle</td>
</tr>
</tbody>
</table>
## Registry keys for 64-bit machines:

<table>
<thead>
<tr>
<th>Registry key</th>
<th>Value</th>
<th>Key path</th>
</tr>
</thead>
<tbody>
<tr>
<td>WSCSupported</td>
<td>True</td>
<td>• HKEY_CURRENT_USER\SOFTWARE\Citrix\Dazzle</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• HKEY_CURRENT_USER\SOFTWARE\Citrix\Receiver\SR\Store</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\Policies\Citrix\Dazzle</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\Citrix\Dazzle</td>
</tr>
<tr>
<td>WSCReconnectAll</td>
<td>True</td>
<td>• HKEY_CURRENT_USER\SOFTWARE\Citrix\Dazzle</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• HKEY_CURRENT_USER\SOFTWARE\Citrix\Receiver\SR\Store</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\Policies\Citrix\Dazzle</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\Citrix\Dazzle</td>
</tr>
<tr>
<td>WSCReconnectMode</td>
<td></td>
<td>• HKEY_CURRENT_USER\SOFTWARE\Citrix\Dazzle</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• HKEY_CURRENT_USER\SOFTWARE\Citrix\Receiver\SR\Store&quot;+ primaryStoreID +&quot;\Properties</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\Policies\Citrix\Dazzle</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\Citrix\Dazzle</td>
</tr>
<tr>
<td>WSCReconnectModeUser</td>
<td></td>
<td>Registry is not created during installation.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• HKEY_CURRENT_USER\SOFTWARE\Citrix\Dazzle</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• HKEY_CURRENT_USER\SOFTWARE\Citrix\Receiver\SR\Store&quot;+ primaryStoreID +&quot;\Properties</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\Policies\Citrix\Dazzle</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\Citrix\Dazzle</td>
</tr>
</tbody>
</table>

## 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**

![Add Account dialog](image)
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.

![Message](image)

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

- **Renaming Citrix execution file:**
  Rename the `CitrixWorkspaceApp.exe` to `CitrixWorkspaceWeb.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 **Add Account** dialog 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.
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 Configuring email based account discovery.
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 Virtual Apps and Desktops Services 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 “HRAapps” has remote access enabled for server2.com, a user must enter server1.com?SalesApps to access SalesApps or enter server2.com?HRAapps to access HRAapps. 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 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.

© 1999-2019 Citrix Systems, Inc. All rights reserved.
**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:

<table>
<thead>
<tr>
<th>Client drive letter</th>
<th>Is accessed by the server as:</th>
</tr>
</thead>
<tbody>
<tr>
<td>A</td>
<td>A</td>
</tr>
<tr>
<td>B</td>
<td>B</td>
</tr>
<tr>
<td>C</td>
<td>V</td>
</tr>
<tr>
<td>D</td>
<td>U</td>
</tr>
</tbody>
</table>
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:

<table>
<thead>
<tr>
<th>Client drive letter</th>
<th>Is accessed by the server as:</th>
</tr>
</thead>
<tbody>
<tr>
<td>A</td>
<td>A</td>
</tr>
<tr>
<td>B</td>
<td>B</td>
</tr>
<tr>
<td>C</td>
<td>C</td>
</tr>
<tr>
<td>D</td>
<td>D</td>
</tr>
</tbody>
</table>

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

March 22, 2019
When using Citrix Workspace app for Windows, the following configurations allow you to access their hosted applications and desktops.

Adaptive transport

Adaptive transport is a data transport mechanism that 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.

With session reliability enabled, EDT, and TCP are attempted in parallel during the initial connection, 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 required to enable the feature using Citrix Studio.
- StoreFront 3.8.
- IPv4 VDAs only. IPv6 and mixed IPv6 and IPv4 configurations are not supported.
- Add firewall rules to allow inbound traffic on UDP ports 1494 and 2598 of the VDA.

Note:
TCP ports 1494 and 2598 are also required and opened automatically when you install the VDA. However, UDP ports 1494 and 2598 are not automatically opened. Set them to Enabled.

Adaptive transport must be configured on the VDA by applying the policy before it is available for communication between the VDA and Citrix Workspace app.

Citrix Workspace app allows the adaptive transport by default. However, also by default, the client attempts to use adaptive transport only if the VDA is configured to Preferred in the Citrix Studio policy 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.

To disable adaptive transport on a specific client, set the EDT options appropriately using the Citrix Workspace app for Windows Group Policy Object administrative template.

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 gedit.msc.
2. Under the Computer Configuration node, go to Administrative Templates > Citrix Workspace > Network routing.
3. Set the Transport protocol for Receiver policy to Enabled.
4. Select Communication Protocol for Citrix Workspace as required.
Citrix Workspace app for Windows

- **Off** - Indicates that TCP is used for data transfer.
- **Preferred** - Indicates that the Citrix Workspace app for Windows tries to connect to the server using UDP at first and then 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.

Also, for the adaptive transport configuration to take effect, add the Citrix Workspace app template files to the **Policy Definitions** folder. For more information on adding template files to the local GPO, see **Group Policy Object template**.

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**

Starting with Version 4.10, 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. Doing so 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 Files
  - 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 Advanced Preferences** policy.
4. Select **Enabled** to hide the Advanced Preferences option from the right-click menu of the Citrix Workspace app icon in the notification area.

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

**Hiding specific settings from the Advanced Preferences sheet**

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

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:

<table>
<thead>
<tr>
<th>Options</th>
<th>Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>Not Configured</td>
<td>Displays the setting</td>
</tr>
<tr>
<td>Enabled</td>
<td>Hides the setting</td>
</tr>
<tr>
<td>Disabled</td>
<td>Displays the setting</td>
</tr>
</tbody>
</table>

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

- Configuration checker
- Connection Center
- High DPI
- Data collection
Citrix Workspace app for Windows

- Delete saved passwords
- Keyboard and Language bar
- Shortcuts and Reconnect
- Support information
- Citrix Files
- 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:
   a) **True** - Displays the Reset Workspace option in the Advanced Preferences sheet.
   b) **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, consider the following options to enhance the user experience:

- **Web Access Mode** - Without any configuration, Citrix Workspace app provides browser-based access to applications and desktops. You can open a browser to a Workspace for Web 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 Workspaces app allows you to select the applications to display in the Start menu.

• App shortcut-only mode - As a Citrix Workspace app for Windows administrator, you can configure Citrix Workspace app to automatically place application and desktop shortcuts directly in the Start menu or on the desktop in a similar way that Citrix Workspace app Enterprise places them. The new *shortcut only* mode allows you to find all the published apps within the familiar Windows navigation schema where you would expect to find them.

For information on delivering applications using Citrix Virtual Apps and Desktops 7, see [Create a Delivery Group application](#).

**Configure self-service mode**

By simply adding a StoreFront account to Citrix Workspace app or configuring Citrix Workspace app to point to a StoreFront site, you can configure self-service mode, which 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
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.

- 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.
Citrix Workspace app for Windows

- To not create an entry on the clients ‘add/remove programs’, use `DontCreateAddRemoveEntry`. Settings: “true” or “false” (default is false).
- To remove shortcuts and Citrix Workspace icon for an application that was previously available from the Store but now is not available, use `SilentlyUninstallRemovedResources`. Settings: “true” or “false” (default is false).

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

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

The section ends with the `</account>` tag.

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

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

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

```xml
<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:

```xml
<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.
Citrix Workspace app for Windows

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 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.
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.
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 a number of 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 back up the registry before you edit it.

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

1. On a client machine, create stub executables for all 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:

<table>
<thead>
<tr>
<th>If you want the user to choose the applications they want in their Start Menu..</th>
<th>configure Citrix Workspace app in self-service mode. In this mode you also configure auto-provisioned and mandatory app keyword settings as needed.</th>
</tr>
</thead>
<tbody>
<tr>
<td>If you want the user to choose the applications they want in their Start Menu but also want specific app shortcuts on the desktop..</td>
<td>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.</td>
</tr>
</tbody>
</table>

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.

<table>
<thead>
<tr>
<th>Option</th>
<th>Configuration</th>
</tr>
</thead>
<tbody>
<tr>
<td>If you want Citrix Workspace app to put all application shortcuts in the start menu automatically..</td>
<td>configure Citrix Workspace app with SelfServiceMode =False. All available apps appear in the Start Menu.</td>
</tr>
<tr>
<td>If you want all application shortcuts to put on desktop..</td>
<td>configure Citrix Workspace app with PutShortcutsOnDesktop = true. All available apps appear in the desktop.</td>
</tr>
<tr>
<td>If you want all shortcuts to be put on the desktop in a folder…</td>
<td>configure Citrix Workspace app with DesktopDir=Name of the desktop folder where you want applications.</td>
</tr>
</tbody>
</table>

### 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:

<table>
<thead>
<tr>
<th>Option</th>
<th>Configuration</th>
</tr>
</thead>
<tbody>
<tr>
<td>If you want per-app settings to determine where applications are placed independently of whether in self-service mode or Start Menu mode..</td>
<td>configure Citrix Workspace app with PutShortcutsInStartMenu=false and enable per app settings.</td>
</tr>
</tbody>
</table>

### Apps in category folders or in specific folders

If you want applications displayed in specific folders use the following options:

<table>
<thead>
<tr>
<th>Option</th>
<th>Configuration</th>
</tr>
</thead>
<tbody>
<tr>
<td>If you want the application shortcuts Citrix Workspace app places in the start menu to be shown in their associated category (folder)..</td>
<td>configure Citrix Workspace app with UseCategoryAsStartMenuPath=True.</td>
</tr>
</tbody>
</table>
Citrix Workspace app for Windows

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.

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.

<table>
<thead>
<tr>
<th>KEYWORDS:prefer=</th>
<th>Shortcut under Programs</th>
<th>Matches?</th>
</tr>
</thead>
<tbody>
<tr>
<td>Word</td>
<td>\Microsoft Office\Microsoft Word 2010</td>
<td>Yes</td>
</tr>
<tr>
<td>Microsoft Word</td>
<td>\Microsoft Office\Microsoft Word 2010</td>
<td>Yes</td>
</tr>
<tr>
<td>Console</td>
<td>McAfee\VirusScan Console</td>
<td>Yes</td>
</tr>
<tr>
<td>Virus</td>
<td>McAfee\VirusScan Console</td>
<td>No</td>
</tr>
<tr>
<td>Console</td>
<td>McAfee\VirusScan Console</td>
<td>Yes</td>
</tr>
</tbody>
</table>
• 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.

<table>
<thead>
<tr>
<th>KEYWORDS:prefer=</th>
<th>Shortcut under Programs</th>
<th>Matches?</th>
</tr>
</thead>
<tbody>
<tr>
<td>\Programs\Microsoft Office\Microsoft Word 2010</td>
<td>\Programs\Microsoft Office\Microsoft Word 2010</td>
<td>Yes</td>
</tr>
<tr>
<td>\Microsoft Office</td>
<td>\Programs\Microsoft Office\Microsoft Word 2010</td>
<td>No</td>
</tr>
<tr>
<td>\Microsoft Word 2010</td>
<td>\Programs\Microsoft Office\Microsoft Word 2010</td>
<td>No</td>
</tr>
<tr>
<td>\Programs\Microsoft Word 2010</td>
<td>\Programs\Microsoft Word 2010</td>
<td>Yes</td>
</tr>
</tbody>
</table>

• 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.

<table>
<thead>
<tr>
<th>KEYWORDS:prefer=</th>
<th>Shortcut under Programs</th>
<th>Matches?</th>
</tr>
</thead>
<tbody>
<tr>
<td>\Microsoft Office\Microsoft Word 2010</td>
<td>\Microsoft Office\Microsoft Word 2010</td>
<td>Yes</td>
</tr>
<tr>
<td>\Microsoft Office</td>
<td>\Microsoft Office\Microsoft Word 2010</td>
<td>No</td>
</tr>
<tr>
<td>\Microsoft Word 2010</td>
<td>\Microsoft Office\Microsoft Word 2010</td>
<td>Yes</td>
</tr>
<tr>
<td>\Microsoft Word</td>
<td>\Microsoft Word 2010</td>
<td>No</td>
</tr>
</tbody>
</table>
Citrix Workspace app for Windows

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.

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 are the days 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 actually 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.

**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 gedit.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.

4. Edit the settings.

   **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.

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

6. 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.

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 Citrix Virtual Apps and Desktops session. The required components are installed with the plug-in. You can enable the Bloomberg keyboard feature when installing Citrix Workspace app for Windows or by using the Registry editor.

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.
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 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
Citrix Workspace app for Windows

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.
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 is 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 gedit.msc.
2. Under the **User Configuration node**, go to **Administrative Templates > Citrix Components > Citrix Workspace > Remoting client devices > Generic USB Remoting**.
3. Select the **SplitDevices** policy.
4. Select **Enabled**.
5. Click **Apply** 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 gedit.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**.

![Desktop Viewer](image)

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

![Connection Center](image)

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

**To allow an interface:**

<table>
<thead>
<tr>
<th>Split</th>
<th>Interface</th>
<th>Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>TRUE</td>
<td>Valid number 0 -n</td>
<td>Allow specified interface</td>
</tr>
<tr>
<td>TRUE</td>
<td>Invalid number</td>
<td>Allow all interfaces</td>
</tr>
<tr>
<td>FALSE</td>
<td>Any value</td>
<td>Allow Generic USB of parent device</td>
</tr>
<tr>
<td>Not specified</td>
<td>Any value</td>
<td>Allow Generic USB of parent device</td>
</tr>
</tbody>
</table>
For example, SplitDevices- true indicates that all devices split.

To deny an interface:

<table>
<thead>
<tr>
<th>Split</th>
<th>Interface</th>
<th>Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>TRUE</td>
<td>Valid number 0 -n</td>
<td>Deny specified interface</td>
</tr>
<tr>
<td>TRUE</td>
<td>Invalid number</td>
<td>Deny all interfaces</td>
</tr>
<tr>
<td>FALSE</td>
<td>Any value</td>
<td>Deny Generic USB of parent device</td>
</tr>
<tr>
<td>Not specified</td>
<td>Any value</td>
<td>Deny Generic USB of parent device</td>
</tr>
</tbody>
</table>

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**.

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.

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 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, 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`.

- 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`.

© 1999-2019 Citrix Systems, Inc. All rights reserved.
Citrix Workspace app for Windows

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.

If you have disabled generic client IME using the command line interface, you can enable the feature again by running the `wfica32.exe /localgenericime:on` command.

**Toggle:**

Citrix Workspace app supports toggle functionality for this feature. You can run the `wfica32.exe /localgenericime:on` command to enable or disable the feature. However, the keyboard layout synchronization settings take precedence over the toggle switch. If keyboard layout synchronization is set to Off, toggling does not enable generic client IME.

**Configure generic client IME using the graphical user interface:**
Citrix Workspace app for Windows

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.

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:

© 1999-2019 Citrix Systems, Inc. All rights reserved.
Citrix Workspace app for Windows

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 clear **Enable Protected Mode**.

**H.265 video encoding**

Citrix Workspace app supports the use of the H.265 video codec for hardware acceleration of remote graphics and videos. 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 Citrix Workspace app to use 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 the Knowledge Center articleCTX135817.

Keyboard layout and language bar

Keyboard layout
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.

   ![Keyboard and Language bar dialog](image)

   **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
**Citrix Workspace app for Windows**

`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 new 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\icalme, 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.
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. 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 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 Citrix 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. 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 Citrix 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:

<table>
<thead>
<tr>
<th>Feature</th>
<th>Client drive mapping</th>
<th>USB support</th>
</tr>
</thead>
<tbody>
<tr>
<td>Enabled by default</td>
<td>Yes</td>
<td>No</td>
</tr>
<tr>
<td>Read-only access configurable</td>
<td>Yes</td>
<td>No</td>
</tr>
<tr>
<td>Safe to remove device during a session</td>
<td>No</td>
<td>Yes, if the user clicks Safely Remove Hardware in the notification area</td>
</tr>
</tbody>
</table>

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 Citrix 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.
Some specialty devices (for example, VOIP phones) require additional configuration. For more information, see Knowledge Center article CTX123015.

- **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.

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.

This class of device (in particular printers with scanning functions) requires additional configuration. For instructions on this, see Knowledge Center article CTX123015.

- **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. For instructions on this, see Knowledge Center article CTX123015.

- **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 proto-
  cols 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 desk-
  top 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 StoreFront 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.

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”.

Content Collaboration Service integration in Citrix Workspace app

This release introduces integration of Citrix Content Collaboration Service with Citrix Workspace app. Citrix Content Collaboration enables you to easily and securely exchange documents, send large documents by email, securely handle document transfers to third parties, and access a collaboration space. Citrix Content Collaboration provides many ways to work, including a web-based interface, mobile clients, desktop apps, and integration with Microsoft Outlook and Gmail.

You can access Citrix Content Collaboration functionality from the Citrix Workspace app using the Files tab displayed within Citrix Workspace app. You can view the Files tab only if Content Collaboration Service is enabled in the Workspace configuration in the Citrix Cloud console.

Note:

Citrix Content Collaboration integration in Citrix Workspace app is not supported on Windows Server 2012 and Windows Server 2016 due to a security option set in the operating system.

The following image displays example contents of the Files tab of the new Citrix Workspace app:
Limitations:

- Resetting Citrix Workspace app does not cause Citrix Content Collaboration to log off.
- Switching stores in Citrix Workspace app does not cause Citrix Content Collaboration to log off.

Configure download location for Citrix Files using the Registry editor:

1. Launch the Registry editor and navigate to HKEY_CURRENT_USER\Software\Citrix\Dazzle\.
2. Create a String Value key by name DownloadPreference.
3. Copy and paste the preferred download path for Citrix Files to the Value column.
4. If you want a prompt for every download, set the Value column to *.

For information about configuring Citrix Files download location using the Advanced Preferences UI, see Configuring download location using Advanced Preferences in Citrix Workspace app for Windows Help documentation.
**Citrix Workspace app for Windows**

**SaaS apps in Citrix Workspace app**

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.

**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 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, desktops, and files 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.

**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.

For information on how to configure SaaS apps using Access Control Services, see **Access Control documentation**.

**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 touchscreen 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.

For more information, see

[XenServer 7.2 Release Notes](#)

**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
```

<p>| | |</p>
<table>
<thead>
<tr>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Name: RelativeMouse</td>
</tr>
<tr>
<td>2</td>
<td>Type: REG_SZ</td>
</tr>
<tr>
<td>3</td>
<td>Value: True</td>
</tr>
</tbody>
</table>

**Note:**

- The values set in the Registry editor takes 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 located 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:
Citrix Workspace app for Windows

- 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**.
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 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:** 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:** 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 Citrix 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 user device operating system must be able to detect each of the monitors. On Windows platforms, to verify that this detection occurs, on the user device, view the **Settings** tab in the **Display Settings** dialog box 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 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, see Knowledge Center article [CTX115637](https://supportcitrix.com/s/topic/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,
Citrix Workspace app for Windows

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 func-
tionality. 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
gedit.msc.
2. Under the **Computer Configuration node**, go to Administrative Templates> Citrix Compo-
nents > 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.

**Citrix Workspace app 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 Reg-

© 1999-2019 Citrix Systems, Inc. All rights reserved.
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 connections on the same user device.

**Note:**

Use Citrix Workspace app to change the screen resolution on their virtual desktops. You cannot change 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
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 Citrix 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 connections 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\ICA\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)

The Citrix Customer Experience Improvement Program (CEIP) gathers anonymous configuration and usage data from Citrix Workspace app and automatically sends the data to Citrix. This data helps Citrix improve the quality, reliability, and performance of Citrix Workspace.

No user identifiable information is collected from the customer environment with CEIP.
Tip
You can change whether you participate in CEIP using the Citrix Workspace app. You have 7 days to disable CEIP after installation.

To disable CEIP, or to forego participation:

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
2. Select Advanced Preferences.
   The Advanced Preferences window appears.
3. Select Data Collection.
4. Select No, Thanks to disable CEIP or to forego participation.
5. Click Save.

Authenticate

March 12, 2019

To maximize the security of your environment, the connections between Citrix Workspace app and the resources you publish must be secured. You can configure various types of authentication for your Citrix Workspace app, including domain pass-through, smart card, and Kerberos pass-through.

Domain pass-through authentication

Single Sign-on lets you authenticate to a domain and use the Citrix Virtual Apps and Desktops without having to reauthenticate again.

When you log on to Citrix Workspace app, your credentials are passed through to StoreFront, along with the enumerated apps and desktops and Start menu settings. After configuring single sign-on, you can log on to Citrix Workspace app and launch Citrix Virtual Apps and Desktops sessions without having to retype your credentials.

Note:
Single Sign-on is not supported if Citrix Workspace app is connected to Citrix Virtual Apps and Desktops using Citrix Gateway.

You can configure single sign-on on both fresh installation or upgrade setup, using any of the following options:
Citrix Workspace app for Windows

- Command line interface
- Graphical user interface

Configure single sign-on during fresh installation

To configure single sign-on during fresh installation of Citrix Workspace app, perform the following steps:

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 the Web Interface

Depending on the Citrix Virtual Apps and Desktops deployment, single sign-on authentication 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:

<table>
<thead>
<tr>
<th>Use case</th>
<th>Configuration details</th>
<th>Additional information</th>
</tr>
</thead>
<tbody>
<tr>
<td>Configured SSON on StoreFront or Web Interface</td>
<td>Launch Citrix Studio, go to Store &gt; Manage Authentication methods &gt; enable Domain pass-through.</td>
<td>When Citrix Workspace app is not configured with Single Sign-on, it automatically switches the authentication method from Domain pass-through to Username and Password, if available.</td>
</tr>
<tr>
<td>When Workspace for Web is required</td>
<td>Launch Store &gt; Workspace for Websites &gt; Manage Authentication methods &gt; enable Domain pass-through.</td>
<td>When Citrix Workspace app is not configured with Single Sign-on, it automatically switches the authentication method from Domain pass-through to Username and Password, if available.</td>
</tr>
</tbody>
</table>
## Use case | Configuration details | Additional information
--- | --- | ---
When StoreFront is not configured | If Web Interface is configured on a Citrix Virtual Apps and Desktops server, launch XenApp Services Sites > Authentication Methods > enable **Pass-through**. | When Citrix Workspace app is not configured with single sign-on, it 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, 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 Explorer.
   b) Select **Tools > Internet Options > 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:
Citrix Workspace app for Windows

a) Launch Internet Explorer.
b) On the Internet Options > Security tab, click 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.

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 to complete the installation.

You can now log on to an existing Store (or configure a new Store) 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 gedit.msc.
2. Under the Computer Configuration node, go to Administrative Template > Citrix Component > Workspace for Windows > 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 the 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**

Complete the following steps to configure Citrix Workspace app for pass-through authentication using Active Directory group policy. In this scenario, you can achieve the single sign-on authentication without using the enterprise software deployment tools, such as Microsoft System Center Configuration Manager.

1. Download and place the Citrix Workspace app installation file (**CitrixWorkspaceApp.exe**) on a suitable network share. It must be accessible by the target machines you install Citrix Workspace app on.

2. Get the **CheckAndDeployWorkspacePerMachineStartupScript.bat** template from the *Citrix Workspace app for Windows Download* page.

3. Edit the content to reflect the location and the version of **CitrixWorkspaceApp.exe**.

4. In the **Active Directory Group Policy Management** console, enter **CheckAndDeployWorkspacePerMachineStartupScript.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](image)

**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.
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, irrespective of pass or fail.

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.

Note:
- If you are accessing Workspace for Web, the test results are not applicable.
- If Citrix Workspace app is configured with multiple stores, the authentication method test runs on all the configured stores.
- You can save the test results as reports. The default report format is .txt.

Hide the Configuration Checker option from the Advanced Preferences window

1. Open the Citrix Workspace app Group Policy Object administrative template by running gpedit.msc.
2. Go to Citrix Components > Workspace for Windows > 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 Citrix Virtual Apps and Desktops servers.

Beacon test
Citrix Workspace app allows you to perform a beacon test using the Beacon checker that is available as part of the Configuration Checker utility. Beacon test helps to confirm if the beacon (ping.citrix.com) is reachable. This diagnostic test helps to eliminate one of the many possible causes for slow resource
Citrix Workspace app for Windows

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.

**Note:**

- The test results are not applicable on Workspace for Web.
- The test results can be saved as reports. The default format for the report is .txt.

**Domain pass-through authentication with Kerberos**

This topic applies only to connections between Citrix Workspace app for Windows and StoreFront, Citrix Virtual Apps and Desktops.

Citrix Workspace app supports Kerberos for domain pass-through authentication for deployments that use smart cards. Kerberos is one of the authentication methods included in Integrated Windows Authentication (IWA).

When enabled, Kerberos authenticates without passwords for Citrix Workspace app. 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 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 Workspace app with information about available the Citrix Virtual Apps and Desktops.

**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 (previously referred to as the ICA client) passes the smart card PIN to the VDA to log the user on to Citrix Workspace app session. Citrix Virtual Apps and Desktops then delivers the requested resources.

To use Kerberos authentication with Citrix Workspace app, ensure 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. 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. Citrix Virtual Apps and Desktops 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 gedit.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.
To configure StoreFront:

When you configure the authentication service on the StoreFront server, select the Domain pass-through option. That setting enables Integrated Windows Authentication. You do not need to select the Smart card option unless you also have non domain-joined clients connecting to StoreFront using smart cards.

For more information about using smart cards with StoreFront, see Configure the authentication service in the StoreFront documentation.

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:
Citrix Workspace app for Windows

- 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 a virtual desktop or application.

Pass-through authentication requires configuration both on StoreFront and Citrix Workspace app.

- **Bimodal authentication** - Bimodal authentication offers users a choice between using a smart card and typing the user name and password. This feature is effective when you 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. When you insert a smart card in a card reader, the certificates are applicable to all applications running on the user device, including Citrix Workspace app.

- **Client certificate authentication** - Client certificate authentication requires Citrix Gateway and StoreFront configuration.
  - For access to StoreFront through Citrix Gateway, you 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 Citrix 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 in non-paged memory only during the user session and is not stored on the disk.
- Citrix Workspace app does not reconnect to a session when a smart card is inserted.
Citrix Workspace app for Windows

- 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 username 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\AuthManager:

`SmartCardPINEntry=CSP`.

**Smart card authentication for Web Interface**

If Citrix Workspace app for Windows is installed with an SSON component, pass-through authentication is enabled by default even if the PIN pass-through for smart card is not enabled on the XenApp PNAgent site; the pass-through setting for authentication methods will no longer be effective. The screen below illustrates how to enable smart card as the authentication method when Citrix Workspace app is properly configured with SSON.

Use the smart card removal policy to control the behavior for smart card removal when a user authenticates to the Citrix Web Interface 5.4 PNAgent site.

When this policy is enabled, the user is logged off from the Citrix Virtual Apps session if the smart card is removed from the client device. However, the user is still logged in to the Citrix Workspace app.
Citrix Workspace app for Windows

For this policy to take effect, the smart card removal policy must be set in the Web Interface XenApp Services site. The settings can be found on Web Interface 5.4, `XenApp Services Site > Pass-through with smart card > Enable Roaming > Logoff the sessions when smart card removed`.

When the smart card removal policy is disabled, the user's Citrix Virtual Apps session is disconnected if the smart card is removed from the client device. Smart card removal on the Web Interface XenApp Services site does not have any effect.

**Note:**
There are separate policies for 32 bit and 64 bit clients. For 32 bit devices, the policy name is `Smartcard Removal Policy (32 Bit machine)` and for 64 bit devices, the policy name is `Smartcard Removal Policy (64 Bit machine)`.

---

**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

March 12, 2019

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.

Citrix Workspace app is compatible with and functions in environments where the Microsoft Specialized Security - Limited Functionality (SSLF) desktop security templates are used. These templates are supported on various Windows platforms.

Deprecated cipher suites

With the release Version 4.12, there are two important changes to the TLS/DTLS secure communications protocols; support for DTLS Version 1.2, and deprecation of TLS/DTLS cipher suites.

DTLS version 1.2 supports the UDP transport protocol, providing the equivalent of TLS version 1.2 for the TCP transport protocol. Previous versions of Citrix Workspace app for Windows already supported TLS version 1.2.
Cipher suites with the prefix `TLS_RSA_` do not offer forward secrecy. These cipher suites are now generally deprecated by the industry. However, to support backward compatibility with older versions of Citrix Virtual Apps and Desktops, Citrix Workspace app for Windows can utilize these cipher suites.

A new Group Policy Object Administrative template has been created to allow usage of the deprecated cipher suites. In Citrix Receiver for Windows Version 4.12, this policy is enabled by default, but does not enforce deprecation of these cipher suites using the AES or 3DES algorithms by default. However, you can modify and use this policy to enforce the deprecation more strictly.

Following is the list of deprecated cipher suites:

- `TLS_RSA_AES256_GCM_SHA384`
- `TLS_RSA_AES128_GCM_SHA256`
- `TLS_RSA_AES256_CBC_SHA256`
- `TLS_RSA_AES256_CBC_SHA`
- `TLS_RSA_AES128_CBC_SHA`
- `TLS_RSA_3DES_CBC_EDE_SHA`
- `TLS_RSA_WITH_RC4_128_MD5`
- `TLS_RSA_WITH_RC4_128_SHA`

Note:
The final two cipher suites use the RC4 algorithm, which is deprecated because these cipher suites are not secure. You might also consider the `TLS_RSA_3DES_CBC_EDE_SHA` cipher suite to be deprecated. You can use this policy to enforce all these deprecations.

For information about configuring DTLS v1.2, see Adaptive transport in Citrix Virtual Apps and Desktops documentation.

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 about adding template files to the local GPO, see 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 gedit.msc
2. Under the Computer Configuration node, go to Administrative Template > Citrix Component > Citrix Workspace > Network Routing.
3. Select the Deprecated cipher suites policy.
4. Select Enabled and choose from the following options:
   a) `TLS_RSA_*`: By default, `TLS_RSA_*` is selected. This option must be selected for you to use the other two cipher suites. The following ciphers suites are included when you select this option:
      i. `TLS_RSA_AES256_GCM_SHA384`
The following table lists the cipher suites in each set:

<table>
<thead>
<tr>
<th>Cipher Suite</th>
<th>Native Crypto Kit mode and cipher set</th>
</tr>
</thead>
<tbody>
<tr>
<td>Open</td>
<td>FIPS</td>
</tr>
<tr>
<td>SP800-52</td>
<td>SP800-52 COM</td>
</tr>
<tr>
<td>SP800-52 GOV</td>
<td>SP800-52 GOV</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Cipher Suite</th>
<th>Open</th>
<th>FIPS ALL</th>
<th>FIPS GOV</th>
<th>FIPS ALL</th>
<th>FIPS GOV</th>
<th>SP800-52</th>
<th>SP800-52 COM</th>
<th>SP800-52 GOV</th>
</tr>
</thead>
<tbody>
<tr>
<td>TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA128 (ii)</td>
<td>Y</td>
<td>Y</td>
<td>Y</td>
<td>Y</td>
<td>Y</td>
<td>Y</td>
<td>Y</td>
<td>Y</td>
</tr>
<tr>
<td>TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA256 (iii)</td>
<td>Y</td>
<td>Y</td>
<td>Y</td>
<td>Y</td>
<td>Y</td>
<td>Y</td>
<td>Y</td>
<td>Y</td>
</tr>
<tr>
<td>TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA (iv)</td>
<td>Y</td>
<td>Y</td>
<td>Y</td>
<td>Y</td>
<td>Y</td>
<td>Y</td>
<td>Y</td>
<td>Y</td>
</tr>
<tr>
<td>TLS_RSA_WITH_AES_128_CBC_SHA (v)</td>
<td>Y</td>
<td>Y</td>
<td>Y</td>
<td>Y</td>
<td>Y</td>
<td>Y</td>
<td>Y</td>
<td>Y</td>
</tr>
<tr>
<td>TLS_RSA_WITH_RC4_128_MD5 (b)</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
</tr>
<tr>
<td>TLS_RSA_WITH_RC4_128_SHA (c)</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
</tr>
<tr>
<td>TLS_RSA_WITH_3DES_CBC_SHA (vi)</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
</tr>
<tr>
<td>TLS_EMPTY_RENEGOTIATION_INFO_CHANGE (vii)</td>
<td>Y</td>
<td>Y</td>
<td>Y</td>
<td>Y</td>
<td>Y</td>
<td>Y</td>
<td>Y</td>
<td>Y</td>
</tr>
</tbody>
</table>

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

### 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. For information about securing Web Interface, see Secure section in the Web Interface 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:
Citrix Workspace app for Windows

- 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.
- 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.
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.

4. Select **Require TLS for all connections** to force Citrix Workspace app to use TLS for all connections to published applications and desktops.

5. From the **Security Compliance Mode** menu, select the appropriate option:
   a) **None** - No compliance mode is enforced.
   b) **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.

c) 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.

6. 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.

7. 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.

8. **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  

9. 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.

10. 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.

11. 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.

12. Use the **Client Certificate** setting to specify the identifying certificate’s thumbprint to avoid prompting the user unnecessarily.

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

The following table lists the cipher suites in each set:

<table>
<thead>
<tr>
<th>Cipher Suite</th>
<th>Native Crypto Kit mode and cipher set</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Open ALL</td>
</tr>
<tr>
<td>TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384()</td>
<td>Y</td>
</tr>
<tr>
<td>TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384()</td>
<td>Y</td>
</tr>
<tr>
<td>TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA</td>
<td>X</td>
</tr>
<tr>
<td>TLS_RSA_WITH_AES_256_GCM_SHA384()</td>
<td>Y</td>
</tr>
<tr>
<td>TLS_RSA_WITH_AES_128_GCM_SHA256()</td>
<td>X</td>
</tr>
<tr>
<td>TLS_RSA_WITH_AES_256_CBC_SHA</td>
<td>X</td>
</tr>
<tr>
<td>TLS_RSA_WITH_AES_128_CBC_SHA</td>
<td>X</td>
</tr>
<tr>
<td>TLS_RSA_WITH_RC4_128_SHA</td>
<td>X</td>
</tr>
<tr>
<td>TLS_RSA_WITH_3DES_EDE_CBC_SHA</td>
<td>X</td>
</tr>
<tr>
<td>TLS_EMPTY_RENEGOTIATION_INFO_SCSV</td>
<td>Y</td>
</tr>
</tbody>
</table>

Notes

1. Ciphersuites that require TLS1.2/TLS1.3
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

<table>
<thead>
<tr>
<th>Source</th>
<th>Type</th>
<th>Port</th>
<th>Details</th>
</tr>
</thead>
<tbody>
<tr>
<td>Citrix Workspace app</td>
<td>TCP</td>
<td>80/443</td>
<td>Communication with StoreFront</td>
</tr>
<tr>
<td>ICA/HDX</td>
<td>TCP</td>
<td>1494</td>
<td>Access to applications and virtual desktops</td>
</tr>
<tr>
<td>ICA/HDX with Session Reliability</td>
<td>TCP</td>
<td>2598</td>
<td>Access to applications and virtual desktops</td>
</tr>
<tr>
<td>ICA/HDX over SSL</td>
<td>TCP</td>
<td>443</td>
<td>Access to applications and virtual desktops</td>
</tr>
<tr>
<td>ICA/HDX from HTML5 Workspace</td>
<td>TCP</td>
<td>8008</td>
<td>Access to applications and virtual desktops</td>
</tr>
<tr>
<td>ICA/HDX Audio over UDP</td>
<td>TCP</td>
<td>16500–16509</td>
<td>Port range for ICA/HDX audio</td>
</tr>
<tr>
<td>IMA</td>
<td>TCP</td>
<td>2512</td>
<td>Independent Management Architecture (IMA)</td>
</tr>
<tr>
<td>Management Console</td>
<td>TCP</td>
<td>2513</td>
<td>Citrix Management Consoles and *WCF services Note: For FMA based platforms 7.5 and later, port 2513 is NOT used.</td>
</tr>
<tr>
<td>Application/Desktop Request</td>
<td>TCP</td>
<td>80/8080/443</td>
<td>XML Service</td>
</tr>
<tr>
<td>STA</td>
<td>TCP</td>
<td>80/8080/443</td>
<td>Secure Ticketing Authority (embedded into XML Service)</td>
</tr>
</tbody>
</table>

**Note:**
In XenApp 6.5 port 2513 is used by XenApp Command Remoting Services through WCF.

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. For more information, see the Web Interface documentation.

**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.

**Citrix Secure Web Gateway**

This topic applies only to deployments using the Web Interface.

You can use the Citrix Secure Web Gateway in either Normal mode or Relay mode to provide a secure channel for communication between Citrix Workspace app for Windows and the server. No Citrix Workspace app configuration is required if you are using the Citrix Secure Web Gateway in Normal mode and users are connecting through the Web Interface.

Citrix Workspace app uses settings that are configured remotely on the server running the Web Interface to connect to servers running the Citrix Secure Web Gateway. See the topics for the Web Interface for information about configuring proxy server settings for Citrix Workspace app.
For more information about configuring proxy server settings, see Web Interface documentation.

If you are using **Relay mode**, the Citrix Secure Web Gateway server functions as a proxy and you must configure Workspace for Windows to use:

- The fully qualified domain name (FQDN) of the Citrix Secure Web Gateway server.
- The port number of the Citrix Secure Web Gateway server.

The FQDN must list, in sequence, the following three components:

- Host name
- Intermediate domain
- Top-level domain

For example: `my_computer.my_company.com` is an FQDN, because it lists, in sequence, a host name (`my_computer`), an intermediate domain (`my_company`), and a top-level domain (`com`). The combination of intermediate and top-level domain (`my_company.com`) is referred to as the domain name.

**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, StoreFront, or Citrix Merchandising Server. 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.

The Citrix merchandising server with Citrix Workspace app enables and configures the launch signature verification using the Citrix Merchandising Server Administrator Console > Deliveries wizard to add trusted certificate thumbprints.

**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.

Elevation level
When User Access Control (UAC) is enabled on devices running Windows 10, Windows 8, Windows 7, only processes at the same elevation/integrity level as `wfcrun32.exe` can launch the virtual applications.

Example 1:
When `wfcrun32.exe` is running as a normal user (unelevated), other processes such as Citrix Workspace app must be running as a normal user to launch applications through `wfcrun32.exe`.

Example 2:
When `wfcrun32.exe` is running in elevated mode, other processes such as Citrix Workspace app, Connection Center, and third party applications using the ICA Client Object that are running in non-elevated mode cannot communicate with `wfcrun32.exe`.

Storebrowse
March 18, 2019

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.
Citrix Workspace app for Windows

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 from a configured store.
- Generate an ICA file by selecting any published Citrix Virtual Apps and Desktops 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:**

<table>
<thead>
<tr>
<th>On a 32 bit machine</th>
<th>[HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\AuthManager\Install]</th>
</tr>
</thead>
<tbody>
<tr>
<td>On a 64 bit machine</td>
<td>[HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\Citrix\AuthManager\Install]</td>
</tr>
</tbody>
</table>

**When Citrix Workspace app is installed by users (non-administrators):**

<table>
<thead>
<tr>
<th>On a 32 bit machine</th>
<th>[HKEY_CURRENT_USER\SOFTWARE\Citrix\AuthManager\Install]</th>
</tr>
</thead>
<tbody>
<tr>
<td>On a 64 bit machine</td>
<td>[HKEY_CURRENT_USER\SOFTWARE\WOW6432Node\Citrix\AuthManager\Install]</td>
</tr>
</tbody>
</table>

**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

<table>
<thead>
<tr>
<th>Windows 10 32-bit and 64-bit editions</th>
</tr>
</thead>
<tbody>
<tr>
<td>Windows 8.1, 32-bit and 64-bit editions</td>
</tr>
<tr>
<td>Windows 7 SP1, 32-bit and 64-bit editions</td>
</tr>
<tr>
<td>Windows Thin PC</td>
</tr>
<tr>
<td>Windows Server 2016</td>
</tr>
<tr>
<td>Windows Server 2012 R2, Standard, and, Datacenter editions</td>
</tr>
<tr>
<td>Windows Server 2012, Standard, and, Datacenter editions</td>
</tr>
<tr>
<td>Windows Server 2008 R2, 64-bit edition</td>
</tr>
<tr>
<td>Windows Server 2008 R2, 64-bit edition</td>
</tr>
</tbody>
</table>

## 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.
Citrix Workspace app for Windows

-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://my.secondexample.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

\storebrowse.exe -l (-M 0x2000 -E)

Description:
Enumerates the available resources

Command example on StoreFront:
\storebrowse.exe -U { Username } -P { Password } -D { Domain } -M 0x2000 -E <https://my.firstexamplestore.net/Citrix/Store/discovery>

Command example on Citrix Gateway:
\storebrowse.exe -U { Username } -P { Password } -D { Domain } -M 0x2000 -E <https://my.secondexamplestore.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/Q2hJk0lmNoPQrSTV9y/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.secondexamplestore.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:

```
```

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:
Citrix Workspace app for Windows


The name that is in bold in the above output will be used as input parameter to the -S option.

Command example on StoreFront:

```bash
\storebrowse.exe -U { Username } -P { Password } -D { Domain } -S "{ Friendly_Resource_Name } <https://my.firstexamplestore.net/Citrix/Store/discovery >
```

Command example on Citrix Gateway:

```bash
\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:

```bash
\storebrowse.exe -f "C:\Temp\Launch.ica" -L "Resource_Name" { Store }
```

Command example on Citrix Gateway:

```bash
\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:

```bash
\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.secondexamplestore.com

**Single Sign-on support with Citrix Gateway**

Single Sign-on lets you authenticate to a domain and use Citrix Virtual Apps and Desktops 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 Citrix Virtual Apps and Desktops enumerated for you, including your Start menu settings. After configuring single sign-on, you can add the store, enumerate the Citrix 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 Citrix 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** (\texttt{-U}), **Password** (\texttt{-P}) and **Domain** (\texttt{-D}) of the Storebrowse utility are case-sensitive and must be in upper case only.

**Citrix Workspace app Desktop Lock**

February 13, 2019

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 required set of options on the toolbar: Ctrl+Alt+Del, Preferences, Devices, and 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 can also be used on non-domain joined machines without SSON enabled. 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.

You must install Citrix Workspace app for Windows with the \texttt{/includeSSON} flag. You must configure the store and Single Sign-on, either using the adm/admx file or cmdline option. For more information, see Install and configure Citrix Receiver using the command line.

Then, install the Citrix Workspace app Desktop Lock as an administrator using the **CitrixWorkspaceDesktopLock.msi** available in the **Citrix Downloads** page.
System requirements

- Microsoft Visual C++ 2005 Service Pack 1 Redistributable Package. For more information, see the Microsoft Download page.
- Supported on Windows 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.
- Domain-joined and non-domain joined end points.
- 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. See Configure Local App Access and URL redirection in Citrix Virtual Apps and Desktops for more information.

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 Viewer toolbar.
- Most windows shortcut keys are passed to the remote session, with the exception of Windows+L. For details, see Passing Windows shortcut keys to the remote session.
- Ctrl+F1 triggers Ctrl+Alt+Del when you disable the connection or desktop viewer for desktop connections.

Install Citrix Workspace app Desktop Lock

This procedure installs Citrix Workspace app for Window so that virtual desktops appear using Citrix Workspace app Desktop Lock. For deployments that use smart cards, see To configure smart cards for use with devices running Receiver Desktop Lock.
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:

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

   For command details, see the Citrix Workspace app install documentation at Configure and install Citrix Workspace for Windows using command-line parameters.

3. In the same folder on the installation media, double-click `CitrixReceiverDesktopLock.msi`. The Desktop Lock wizard appears. Follow the prompts.

4. When the installation completes, restart the user device. If you have permission to access a desktop and you 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 `CitrixWorkspaceDesktopLock.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 for Windows 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 devices running Citrix Workspace app for 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 with smart card is enabled (enabled by default).
   d) Enable Kerberos.
   e) Enable Kerberos and Pass-through 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 Citrix Workspace app 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.
Citrix Workspace app for Windows

- 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

March 12, 2019

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 Citrix 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

August 29, 2018

ICA Settings Reference

The ICA file settings reference provides registry settings and ICA file settings lists, allowing administrators to customize the behavior of Citrix Workspace app. You can also use the ICA Settings Reference to troubleshoot unexpected Citrix Workspace app behavior.