About Citrix Workspace app 2507.1 LTSR for Windows

This documentation describes the features and configuration of Citrix Workspace app 2507.1 LTSR for Windows. This version is the latest Long Term Service Release (LTSR) of Citrix Workspace app for Windows and is relevant only for LTSR customers. The documentation for the Current Release (CR) of Citrix Workspace app for Windows is available at Citrix Workspace app for Windows. For more information about the lifecycles of CRs and LTSRs, see Lifecycle Milestones for Citrix Workspace app.

Note:

- If you have enabled auto-update on your Citrix Workspace app and have opted for the LTSR program, Citrix Workspace app 2507.1 LTSR for Windows automatically updates to Citrix Workspace app 2507.1 LTSR for Windows.
- If you have enabled auto-update on your Citrix Workspace app and have opted for the CR program, await the release of version 2508, after which Citrix Workspace app CR version automatically updates to Citrix Workspace app 2508 for Windows.
- Citrix Workspace app version 2507.1 LTSR is designated as the final version to include official support for Microsoft Windows 10. Following the End-of-Life (EOL) of Windows 10 in October, subsequent Current Release (CR) builds of Citrix Workspace app (such as version 2511) might still be installed on Windows 10 devices. However, Citrix cannot provide official support for operating systems that are no longer supported by Microsoft. While core functionality will continue to be validated during testing, any issues specific to Windows 10 reported after the EOL date will only be addressed on a best-effort basis. In addition, Citrix cannot guarantee compatibility with changes in Microsoft components (for example, .NET Framework or Edge WebView2) that might affect the Citrix Workspace app experience on Windows 10 beyond version 2507.1 LTSR.
- Citrix Enterprise Browser™ can be used with Citrix Workspace™ app LTSR as a compatible component. However, it isn't installed by default. To install Citrix Enterprise

Browser, add install switch `InstallEmbeddedBrowser=Y` or Addlocal parameter `CitrixEnterpriseBrowser` as part of the command-line installation.

- If.NET isn't installed on the system or a version less than 8.0.15 is installed on the system, Citrix Workspace app installs .NET version 8.0.16. If you install any supported higher version of .NET, Citrix Workspace app is compatible with the highest available .NET version (up to 8.x).

Downloads

Citrix Workspace app 2507.1 LTSR for Windows

Note:

Citrix Workspace app for Windows 2507.1 is now available. You can sign in with your account to access the download.

New Add-ons and Packaging

Automated Endpoint Analysis client installation

The Endpoint Analysis client for Windows now automatically installs with Citrix Workspace app, providing significantly easier deployment than previous GACS-only automatic installation options. This auto-installation greatly aids deployment for customers using BYOD and unmanaged devices, streamlining processes for administrators and boosting overall efficiency.

Note:

Starting with Endpoint Analysis client version 25.8.1.2, support for 32-bit systems has been discontinued.

Modular Browser Content Redirection

Starting with the Citrix Workspace app 2507 for Windows, the Browser Content Redirection (BCR) component is now managed as a modular component, separate from the main Citrix Workspace app installer.

This new modular and evergreen model allows the Browser Content Redirection component to be updated independently and uninstalled independently. This feature provides the following key benefits:

- **Enhanced security**: The BCR Chromium Embedded Framework component can receive security patches and updates as soon as they are available, without waiting for a full Citrix Workspace app release.
- **Simplified Management**: Customers no longer need to update entire Citrix Workspace app to receive the latest Browser content redirection features.
- **Accelerated Innovation**: Faster deployment of new BCR features, enhancements, and bug fixes is now possible, delivering continuous value to customers

To ensure a consistent user experience, the Modular BCR component is installed by default in Citrix Workspace app.

> **Note:**
>
> In Citrix Workspace app 2402 LTSR, the BCR component was not installed by default. With Citrix Workspace app 2507 LTSR, BCR has undergone significant user experience improvements and is now installed by default.

> For more information, see Modular Browser Content Redirection.

Simplified distribution of uberAgent® on endpoints through Citrix Workspace app

uberAgent delivers advanced User Experience and Endpoint Security related insights. Starting with 2507 release, uberAgent is now packaged with Citrix Workspace app. This integration supports simplified distribution of uberAgent, streamlining deployment and reducing administrative overhead.

For more information, see uberAgent add-on support for managed devices in Citrix Workspace app.

New features and enhancements

For more information on the new features, fixed issues, and known issues in this release, refer to the following sections.

- Fixed issues in 2507.1 LTSR
- What's new in 2507 LTSR
- Fixed issues in 2507 LTSR
- Known issues in 2507 LTSR

Helpful links

- Citrix Workspace app feature matrix
- Lifecycle Milestones for Citrix Workspace app
- Additional Lifecycle Information for Citrix Receiver for Windows

Citrix product name and number changes

For information about product name and version number changes that were introduced in 2018, see New names and numbers.

Compatible components

The following components are compatible with LTSR environments. They are not eligible for the LTSR benefits (extended lifecycle and fix-only cumulative updates).

COMPATIBLE COMPONENTS AND FEATURES
Citrix Endpoint Analysis
Citrix DaaS (formerly Citrix Virtual Apps and Desktops™ service)
Browser Content Redirection
Citrix Enterprise Browser
uberAgent
DeviceTRUST

What’s new

About this release

Citrix Workspace™ app 2507.1 Cumulative Update 3 (CU3) Hotfix 1 for Windows is the most recent update to the Citrix Workspace app 2507.1 Long Term Service Release (LTSR).

- About 2507.1 LTSR (initial release)
- About 2507.1 LTSR Cumulative Update 1 (CU1)
- About 2507.1 LTSR Cumulative Update 2 (CU2)
- About 2507.1 LTSR Cumulative Update 3 (CU3)

Cumulative Update 3 (CU3)

Cumulative Update 3 (CU3) Hotfix 1

What's new

This release addresses an issue as mentioned at the Fixed issues page.

What's new in Cumulative Update 3 (CU3)

.NET 10 support

This release adds support for the latest .NET 10 runtime. The minimum required .NET runtime version is 10.0.9.

Auto-update migration

This release adds support for auto-update migration from Citrix Workspace app 2507 x86 to the latest x64 CWA. It can be enabled through group policy: **Citrix Workspace Updates > Migrate 32-bit application to a native 64-bit version on 64-bit operating systems**. For more information, see Transition to 64-bit Architecture — FAQ.

Citrix Enterprise Browser

Starting with version 2511, the Citrix Enterprise Browser (CEB) is no longer integrated into the Workspace app installation package. If required, users and administrators can now install CEB independently by downloading it directly from the Citrix Downloads page, located under the Citrix Enterprise Browser section.

2507.1 LTSR CU3 compatible components

The following components at the following given versions are compatible with LTSR environments. They aren't eligible for the LTSR benefits (extended lifecycle and fix-only cumulative updates).

COMPATIBLE COMPONENTS AND FEATURES	VERSION AS SHOWN IN PROGRAMS AND FEATURES	DOCUMENTATION
Citrix Endpoint Analysis	26.5.1.7	Citrix Endpoint Analysis
Browser Content Redirection	26.3.10.54	Browser Content Redirection
DeviceTRUST	26.3.10.43	deviceTRUST
uberAgent	8.0.7535	uberAgent

Fixed issues

Citrix Workspace™ app 2507.1 LTSR CU3 Hotfix 1 fixed issues

- This release includes fixes for publicly disclosed security vulnerabilities . For more information, see Knowledge Center article CTX697181
- "Migrate 32-bit application to a native 64-bit version on 64-bit Operating Systems" GACS policy is not honoured, wherein the same GPO settings were honoured.
- Session launch might fail if the **VirtualDriverEx** registry entry under `HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\Citrix\ICA Client\Engine\Configuration\Advanced\Modules\ICA 3.0` becomes corrupted after installing the Microsoft Teams VDI plug-in.

Citrix Workspace app 2507.1 LTSR CU3 fixed issues

- This release includes fixes for publicly disclosed security vulnerabilities . For more information, see Knowledge Center article CTX697181

Content Redirection

- When using Bi-directional Content Redirection with OAuth-based federated authentication, the authentication result might not transfer back to the VDA session. This can cause the application sign-in to fail.

End User Experience Monitoring

- Wi-Fi statistics might be missing from the session details reported to Citrix Analytics.

HDX Graphics

- Sessions might disconnect intermittently and the client session process might close unexpectedly due to a memory leak during D3D11 video decoding.

HDX Plug and Play

- An USB error prompt might appear when certain USB composite microphone devices are connected.

HDX RealTime

- When sharing screen during Microsoft Teams optimized calls, the launched session might close unexpectedly.

Installing, Uninstalling, Upgrading

- Hidden stores might not be added with commandline or GPO configuration methods. Set the `AddHiddenStoresConfiguredByAdmin` registry value to revert to the previous behavior of adding hidden stores using admin configuration methods.
- On endpoints with .NET 10 already installed, the .NET runtime prerequisite check might be skipped during Citrix Workspace app installation, and a prompt to install the .NET runtime might later appear during session launch.
- On certain Windows 11 23H2 endpoints that also have the VDA installed, the Citrix Workspace app installer might close unexpectedly during initialization before the setup UI appears.
- The stale helper files WindowsAppRHelper_*.dll might remain in the local application data folder.
- On Azure Virtual Desktop endpoints using Microsoft Edge, ICA client detection might fail and ICA files might not launch after web authentication. This might occur when antivirus software deleteswfcwin32.log, which triggers an MSI repair while launching the session.
- Global App Configuration Service settings might not restrict Citrix Workspace app versions.

Logon/Authentication

- Enhanced single sign-on might fail with an error indicating that authentication information for the session could not be found.
- When the Enable_SSON command-line parameter might not be honored during Citrix Workspace app installation, Single Sign-On might not be enabled or disabled as specified.

Memory, CPU Optimization

- When connecting to VDA 2402 CU4 in a hybrid CVAD environment, the `wfica32.exe` process might consume excessive CPU resources on the client endpoint.

Printing

- Network printers configured on the client endpoint might not be mapped inside Citrix Workspace app sessions.
- After installing Citrix Workspace app 2507 CU1, printer enumeration in sessions might be slow.
- Printers created by third-party session-printing tools might no longer appear inside published desktop sessions.
- When an IPP printer is present, published desktops might fail to launch in hybrid environments after upgrading to newer Citrix Workspace app versions.
- Client IPP printers might fail to map inside sessions and the client-printing status might report the printer as not valid.
- IPv6 IPP printers might not be redirected into the session.

Seamless Windows

- Seamless applications might not take focus immediately after launch and therefore might not accept keyboard input. To revert to the legacy focus mode before this fix, set the following registry values on the endpoint machine.
  - **Path**: `HKEY_LOCAL_MACHINE\Software\Wow6432Node\Citrix\ICA Client\Engine\Configuration\Advanced\Modules\WFClient`
  - **Value name**: `TWISeamlessFlag`
  - **Value type**: `REG_SZ`
  - **Value**: `129`

Security Issues

- Citrix Workspace app might ship OpenSSL libraries that are affected by publicly disclosed vulnerabilities, CVE-2025-11187, CVE-2025-15467, CVE-2026-45447. ,
- After installing the May Windows security update, KB5089549 on endpoints running Citrix App Protection, the client machine might become unresponsive.
- This release includes fixes for publicly disclosed security vulnerabilities CVE-2026-78546 and CVE-2026-78547.

Session/Connection

- On every first launch of published application or desktop from a downloaded ICA file, Citrix Workspace app might not upload Always On Tracing logs to the centralized log server.
- On an endpoint where a per-machine Citrix Workspace app is installed on top of per-user install and post automatic clean-up of per-user version. Launching an application might display a continuous spinning indicator, and toast notification related to session launch will be missing. .
- When reachable external beacons are configured as NetScaler Gateway URLs that have Web Application Firewall enabled for portal endpoints, Citrix Workspace app might fail to add stores.
- In double-hop scenarios, published applications on the second-hop VDA might keep focus and prevent switching to other applications unless the current application is minimized.
- Resources might fail to launch, and the client session process might close unexpectedly during session launch when a partial Virtual Store registry path is accessed.
- After upgrading the client operating system to Windows 11 24H2 or 25H2, Citrix Workspace app might fail to authenticate to the store, and applications and desktops might fail to launch. ,
- The Wi-Fi signal strength shown in Citrix Director session performance might differ from the value reported by the Windows client.
- Kiosk endpoints might intermittently fail to reconnect to disconnected sessions.

User Experience

- Citrix Workspace app might display a persistent spinning wheel during sign-in in on-premises deployments.
- After upgrading Citrix Workspace app, copy and paste might not work correctly when using dictation software.

User Interface

- When you configure application shortcut settings through UI from Advance Preference → shortcut and reconnect cannot be changed once it is set through UI.
- Group Policy settings is added for refreshing the Start menu and showing the sign-in page on log off.
- The Desktop Lock preferences link might open the default web browser and bypass the lockdown configuration.

Known issues in 2507.1 LTSR CU3

On an endpoint where a standard user installs an older Citrix Workspace app version as a per-user and later installs the latest version as a per-machine installation, signing in again can automatically start removal of the per-user installation. During removal, `Cleanup.exe` process might close unexpectedly. However, the user-installed version is removed post that and the per-machine installed version functions correctly.

Cumulative Update 2 (CU2)

What's new in Cumulative Update 2 (CU2)

CWA Log Upload Support Through Gateway Scenarios

Citrix Workspace app (CWA) now supports uploading AOT logs in deployments where users connect through Citrix Gateway. Previously, direct log upload was supported only in direct connection scenarios. With this enhancement, customer devices can now forward Citrix Workspace app logs to the configured AOT Log Server even when connections are established through Gateway, enabling improved end-to-end troubleshooting visibility.

To use this capability, customers must use one of the following Citrix Workspace app for Windows versions:

- Citrix Workspace app for Windows 2603 or later
- Citrix Workspace app for Windows 2507 CU2 or later

2507.1 LTSR CU2 compatible components

The following components at the following given versions are compatible with LTSR environments. They aren't eligible for the LTSR benefits (extended lifecycle and fix-only cumulative updates).

COMPATIBLE COMPONENTS AND FEATURES	VERSION AS SHOWN IN PROGRAMS AND FEATURES	DOCUMENTATION
Citrix Endpoint Analysis	25.11.1.8	Citrix Endpoint Analysis
Browser Content Redirection	25.11.1	Browser Content Redirection
DeviceTRUST	25.11.24.0	deviceTRUST
Citrix Enterprise Browser	140.1.1.33	Citrix Enterprise Browser
uberAgent	7.5.1.7185	uberAgent

Note:

uberAgent 7.5.1 and higher versions support only x64 (64-bit) platforms. You cannot install or use uberAgent on x86 (32-bit) machines.

Fixed issues

Citrix Workspace app 2507.1 LTSR CU2 fixed issues

User Experience

- When you disconnect a session on a German locale system, a **Selection not available** pop-up might appear instead of the expected **Disconnect Desktop** prompt.
- When you enable Desktop Lock, the client PC might not shut down after the user shuts down the virtual desktop session.
- When you configure the **DontCreateAddRemoveEntry** registry setting, Citrix published apps might still appear in the Windows **Apps and Features** list. This issue might cause compliance scan failures.

Session/Connection

- When you launch applications by using desktop shortcuts or `selfservice.exe -qlaunch` in Citrix Workspace app 2507 CU1, session establishment might be noticeably slower than in previous versions.

- Users might not be able to connect to a published desktop through Desktop Lock when there is no external network access.
- When you configure a session inactivity timeout in StoreFront Cloud and the machine goes to sleep or hibernates before the timeout, Citrix Workspace app for Windows might not enforce reauthentication after the idle period expires.
- Resources might fail to launch, and the client session process might close unexpectedly during session launch when a partial Virtual Store registry path is accessed.

Installing, Uninstalling, Upgrading

- When you install Citrix Workspace app by using `/cleaninstall`, the installer might unintentionally remove uberAgent even though Citrix Workspace app does not install it.
- When a Citrix Workspace app upgrade fails and the installer retries the installation, it might install Citrix Workspace app in the wrong location.
- Upgrading from Citrix Workspace app versions earlier than 2507 using the `/cleaninstall` might fail to install after uninstalling the earlier version.
- Uninstalling Citrix Workspace app with the latest DeviceTRUST version 25.11 (included in Citrix Workspace app LTSR 2507.1 CU1) might previously leave some DeviceTRUST-related registry keys under `Computer\HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\ICA\Client\Engine\Configuration\Advanced\Mo`

Client Device Issues

- When you plug in or remove a USB keyboard during an active session, keyboard input might stop working on both the client and the server.
- When you make a Microsoft Teams call in a published desktop and take keyboard control from a user, keyboard input might behave unexpectedly in both local and remote sessions.
- On tablet devices that run Citrix Workspace app, only the front camera might appear in Citrix HDX Web Camera. The rear camera might not be available.

System Exceptions

- When you launch sessions, `wfica32.exe` might crash with a "This version of Citrix Workspace does not support selected encryption" error.
- On Windows 10 devices, a Blue Screen of Death (BSOD) might occur after you install or upgrade Citrix Workspace app when certain third-party endpoint protection software is present.

Content Redirection

- When you use host-to-client redirection, you can ignore CRL ping errors on the client. Set the following registry key on the VDA.
  - **Path:** `HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Citrix\Policies`
  - **Name:** `SFTA`
  - **Type:** `REG_DWORD`
  - **Value:** `2`

TWAIN

- When using TWAIN or WIA scanner redirection, you might experience intermittent failures that impact scanning workflows. Users can see errors such as **No scan drivers were detected, "This scanner cannot be used… (Code: 5042436)**, or prompts indicating that the device appears to be in use and cannot be attached. The issue affects both locally attached and network scanners and occurs at logon or during an active session.

Known issues

Known issues in 2507.1 LTSR CU2

- Network printers might fail to map in a virtual session when certain standard network service name entries are missing from the client device's configuration.
- Printers might take longer than expected to appear in virtual sessions after upgrading to Citrix Workspace app for **Windows 2507 CU1 or 2511**.

Cumulative Update 1 (CU1)

What's new in Cumulative Update 1 (CU1)

Always On Tracing support for Citrix Workspace app for Windows

This release introduces Always On Tracing (AOT) support for Citrix Workspace app for Windows. With this enhancement, log collection is automatic and continuous, enabling Workspace app components to generate structured AOT logs that are centrally collected by the AOT Log Server. This approach removes the need for manual log capture or issue reproduction on end-user devices.

AOT logs from the Workspace app are integrated with Citrix Virtual Apps and Desktops (CVAD) AOT data. This integration provides end-to-end visibility into connection, launch, and session workflows, allowing IT teams to correlate client-side and backend events, troubleshoot issues more efficiently, and reduce the time required to collect diagnostic information.

This feature further enhances observability at the Workspace app layer and supports continuous tracing across the Citrix environment. For more information and guidance on getting started, see Always On Tracing.

To enable the feature, add the following registry key:

`HKLM\Software\Wow6432Node\Citrix\Dazzle` Name: `AotLogCollectionEnabled` Type: `REG_SZ` Value: True

2507.1 LTSR CU1 compatible components

The following components at the following given versions are compatible with LTSR environments. They aren't eligible for the LTSR benefits (extended lifecycle and fix-only cumulative updates).

COMPATIBLE COMPONENTS AND FEATURES	VERSION AS SHOWN IN PROGRAMS AND FEATURES	DOCUMENTATION
Citrix Endpoint Analysis	25.10.1.10	Citrix Endpoint Analysis
Browser Content Redirection	25.8.20	Browser Content Redirection
DeviceTRUST	25.11.18.0	deviceTRUST
Citrix Enterprise Browser	140.1.1.33	Citrix Enterprise Browser
uberAgent	7.4.1.6602	uberAgent

Fixed issues

Citrix Workspace app 2507.1 LTSR CU1 fixed issues

Installing, Uninstalling, Upgrading

- Auto-update might fail during download when a PAC or WPAD proxy configuration is in use.

Logon/Authentication

- Enumeration of stores might fail when your device name contains Unicode characters.

- Store addition might result in a white screen when adding a Citrix Gateway store with a hostname containing **citrixng**.
- Entra ID SSO might not disable as expected even when you set the `AllowSSOForEdgeWebview` registry value in `Computer\HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\Citrix\Dazzle` to false.

Session/Connection

- You might experience random authentication failures when you connect to published apps or desktops through a Citrix Gateway store.
- You might be unable to launch published apps through a browser opened as a standard user while logged into the endpoint as an admin user.
- Starting with Citrix Workspace app for Windows 2507, Storebrowse returns an HTTP 400 error code when attempting to download ICA files from Citrix StoreFront 2507 and later.

System Exceptions

- You might encounter wfica32.exe becoming unresponsive in double-hop scenarios due to latency calculation errors.
- You might see wfica32.exe become unresponsive when connecting to VMs with printer names containing multibyte characters.
- Citrix Workspace app might block Dell Optimizer from monitoring registry values.

Printing

- A popup saying **Please wait for printer connection or cancel connection** might appear after launching a published desktop if a connected IPP printer is offline.
- Printing large files to pdf might fail.

Seamless Windows

- The system tray icon menu might not work as expected, and seamless app window focus may behave inconsistently.

Client Device Issues

- The CtxUsbDiagnostics tool may display **JSON data is corrupt** on some devices that include unprintable control characters.

TWAIN

- You might not be able to scan after pressing Ctrl+F1 or Ctrl+Alt+Del when the published app is in focus.

Known issues

Known issues in 2507.1 LTSR CU1

- Upgrading from Citrix Workspace app versions earlier than 2507 using the `/cleaninstall` might fail to install after uninstalling the earlier version. As a workaround, use `/cleaninstall /silent` to upgrade. This issue is fixed in 2507.1 LTSR CU2.
- When you configure application shortcut settings through UI from **Advance Preference** → **shortcut and reconnect** cannot be changed once it is set through UI. As a workaround, reset Citrix Workspace app or use Application Shortcuts through Group Policy Objects or Global App Configuration Service.
- With the latest DeviceTRUST version 25.11 included in Citrix Workspace app LTSR 2507.1 CU1, uninstalling Citrix Workspace app might leave some DeviceTRUST-related registry keys under `Computer\HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\ICA\Client\Engine\Configuration\Advanced\Mo` This issue is fixed in 2507.1 LTSR CU2.

Citrix Workspace™ app 2507.1 LTSR for Windows

Learn about new features and enhancements available for Citrix Workspace app 2507.1 LTSR for Windows.

> **Important:**

> Citrix Enterprise Browser™ do not get Citrix Workspace app LTSR benefits (extended lifecycle and fix-only cumulative updates) as it isn't LTSR compliant. However, it is allowed to be used with Citrix Workspace app LTSR as compatible component. You must know that Citrix Workspace app LTSR includes current release updates for this component. Also, Citrix Enterprise Browser isn't installed by default, as it is considered optional.

> Starting with LTSR 2507.1, Citrix Workspace App for Windows supports Arm64 devices in emulation mode. App Protection in this configuration can be leveraged to block screen

> capture attempts of sensitive content in protected applications by AI Agents like Microsoft Recall.

What's new in 2507.1 LTSR

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

What's new in 2507 LTSR

The following is a list of features that are available in Citrix Workspace app 2507 LTSR for Windows.

- 2507 LTSR
  - Citrix Troubleshoot Connection
  - Extends long-term support to Windows 11 IoT enterprise LTSC
  - Automated Endpoint Analysis client installation
  - Service continuity enabled without self-service mode
  - Enhanced session timeout enforcement on citrix Gateway
  - Enhanced storebrowse session handling
  - Support for GACS claimed URLs for the US Gov region
  - Automated sign-out on session disconnect
  - ADMX file import support for Intune
  - Modular Browser Content Redirection
  - Zoom 64-bit plug-in management support
  - Simplified distribution of uberAgent® on endpoints through Citrix Workspace app
  - Enhanced background blur persistence for webcam
  - Enhanced keyboard layout settings notification
  - Enable noise suppression
  - Version upgrade for Chromium Embedded Framework
  - Citrix Enterprise Browser
  - App Protection support for ARM64 on devices
  - Browser Profile Sharing
  - HDX graphics superresolution upscaling

- 2503.10
  - Audio Quality Enhancer to improve audio performance
  - Schedule automatic update using GACS
- 2503
  - Client-side graphics optimizations
  - Persistent session in Citrix Workspace app
  - Enhanced Desktop Viewer toolbar
  - Enhancement to connection strength indicator on Desktop Viewer toolbar
  - Multi-monitor layout selection
  - Enhancements on Desktop Lock or Boot to VDI feature
  - Simplified SSON
  - Seamless integration of deviceTRUST® with Citrix Workspace app
  - Enhancement to auto-update
  - Enable auto-update for active users only
  - Enhanced installation process for Citrix Workspace app with App Protection
  - Improved installation process for Citrix Workspace app
  - Auto-sync backend resource changes for Start menu and Desktop shortcuts
  - Install Zoom and Webex plug-in managers during Citrix Workspace app installation
  - Log collection support for non-admin users
  - Enhanced security and compatibility with AppLocker
  - Improved audio performance in Microsoft Teams
  - Monitor third-party UC app optimization status using Citrix Director
  - Hybrid launch support using GACS for on-premises stores
  - Hybrid launch support using GACS for cloud stores - Technical Preview
  - Browser Profile Sharing - Technical Preview
  - Enable noise suppression - Technical Preview
  - Screen recording for specific applications - Technical Preview
- 2409
  - Support for Windows 11 24H2

- Feature flag management
- Single sign-on support for Edge WebView when using Microsoft Entra ID
- Enhanced virtual desktop screen resizing experience
- Enhanced desktop launch experience
- Enhancement to sustainability initiative
- Streamlined beacon checks
- .NET requirements
- SOCKS5 proxy support for EDT
- Customization of Desktop Viewer toolbar
- Remember USB connections
- Disabling the “Exiting Full Screen Mode” tip prompt
- Support for WebHID API in UCSDK
- Support for TLS protocol version 1.3
- Disabling TLS 1.0 or 1.1 communication protocols
- Default audio device selection
- Connection Strength Indicator on Desktop Viewer toolbar
- Enable Audio Quality Enhancer to improve audio performance (Technical Preview)
- Virtual Channel Plugin Manager
- Deprecation of PNAgent-based stores

- 2405
  - Compatibility with the higher versions of .NET
  - Single sign-on support for ARM64-based devices
  - New Add-ons and packaging
  - Configure store names for your store URL
  - Improved Beacon checker tool
  - Option to prevent endpoint from going to sleep when a session is active
  - Enhancement to relative mouse
  - Share system audio
  - Upgraded version of WebRTC for the optimized Microsoft Teams

    - Support for MJPEG webcams
    - Enhanced System Logs for browser content redirection
    - Browser Content Redirection and Microsoft Teams Optimization support for ARM64 based devices[Technical Preview]
    - App Protection support for double-hop scenario
    - Citrix Enterprise Browser
        - Modify the user-agent of Citrix Enterprise Browser
        - Additional security restrictions for the Citrix Enterprise Browser

- 2403
    - Sustainability initiative for cloud hybrid launch
    - Enhanced domain pass-through for single sign-on (Enhanced SSO)
    - Support for advanced NetScaler® policies for Storebrowse on Windows
    - Install Microsoft Teams VDI plug-in for Citrix
    - Hide Troubleshooting and Send Feedback options for end users
    - Deprecation of PNAgent support
    - App Protection
        - Screen Capture Allow List
        - Process exclusion list
        - USB Filter Driver Exclusion List
    - Citrix Endpoint Analysis
    - Citrix Enterprise Browser
        - Security indicator when visiting websites
        - (#Citrix Enterprise Browser introduces additional settings in the Global App Configuration service)

2507 LTSR features

> **Note:**

- Citrix Workspace app for Windows 2507 is now available. You can sign in with your account to access the download.
- Citrix Workspace app version 2507 LTSR is designated as the final version to include official support for Microsoft Windows 10. Following the End-of-Life (EOL) of Windows 10 in October, subsequent Current Release (CR) builds of Citrix Workspace app (such as version 2511) might still be installed on Windows 10 devices. However, Citrix cannot provide official support for operating systems that are no longer supported by Microsoft. While core functionality will continue to be validated during testing, any issues specific to Windows 10 reported after the EOL date will only be addressed on a best-effort basis. In addition, Citrix cannot guarantee compatibility with changes in Microsoft components (for example, .NET Framework or Edge WebView2) that might affect the Citrix Workspace app experience on Windows 10 beyond version 2507 LTSR.
- Citrix Enterprise Browser can be used with Citrix Workspace app LTSR as a compatible component. However, it isn't installed by default. To install Citrix Enterprise Browser, add install switch `InstallEmbeddedBrowser=Y` or Addlocal parameter `CitrixEnterpriseBrowser` as part of the command-line installation.
- If.NET isn't installed on the system or a version less than 8.0.15 is installed on the system, Citrix Workspace app installs .NET version 8.0.16.
- If you install any supported higher version of .NET, Citrix Workspace app is compatible with the highest available .NET version (up to 8.x).

Citrix Troubleshoot Connection

Citrix empowers end users to self-troubleshoot desktop or app launch failures. The system provides recommendations to fix issues. Users can execute fixes with a single button click. Enhanced error messages help users understand launch failure causes clearly.

The Citrix Troubleshoot Connection feature analyzes VDA reachability challenges during launch. It provides user-friendly error messages in real time during failures. The feature offers recommendations to fix issues or collect logs for support tickets.

For more information, see Citrix Troubleshoot Connection.

Extends long-term support to Windows 11 IoT enterprise LTSC

Citrix Workspace app for Windows now supports Windows 11 IoT Enterprise Long-Term Servicing Channel (LTSC), offering vital stability and reliability for these devices. This crucial enhancement supports fixed-function, special-purpose devices, ensuring a 10-year long-term support lifecycle,

providing essential and lasting stability. This support particularly benefits industries like banking, quick-service restaurants, healthcare, hospitality, manufacturing, and retail, requiring consistent equipment operation.

Automated Endpoint Analysis client installation

The Endpoint Analysis client for Windows now automatically installs with Citrix Workspace app, providing significantly easier deployment than previous GACS-only automatic installation options. This auto-installation greatly aids deployment for customers using BYOD and unmanaged devices, streamlining processes for administrators and boosting overall efficiency.

> **Note:**
>
> Starting with Endpoint Analysis client version 25.8.1.2, support for 32-bit systems has been discontinued.

Service continuity enabled without self-service mode

Disabling self-service mode removes the user interface, allowing users to launch applications and desktops exclusively through shortcuts.

Service continuity is now supported even when self-service mode is disabled in Citrix Workspace app for Windows.

Enhanced session timeout enforcement on citrix Gateway

Starting with Citrix Workspace app for Windows version 2507, session timeout enforcement on the gateway has been improved. Previously, background refresh calls from the Citrix Workspace app might cause the Citrix Gateway to extend session timeouts, even when there was no actual user activity.

Enhanced storebrowse session handling

Starting with this release, storebrowse' session handling is improved with the following enhancements, optimizing user experience and critical resource management within high-availability environments to boost efficiency:

- Storebrowse intelligently ignores existing sessions when launching virtual applications
- Storebrowse API support for returning session lists

For more information, see Enhanced storebrowse session handling.

Support for GACS claimed URLs for the US Gov region

Starting with version 2507, Citrix Workspace app supports discovery of Global App Config Service (GACS) claimed URLs for the US Gov region alongside commercial cloud deployments.

You can select the region from which Citrix Workspace app retrieves discovery endpoints using the GACS Discovery Region policy setting.

For more information, see Support for GACS claimed URLs for the US Gov region.

Automated sign-out on session disconnect

Beginning with this release, Citrix Workspace app can automatically sign out users when their session is disconnected. This feature is designed for kiosk environments to enhance security on shared devices.

You can enable this feature through Group Policy Object (GPO) or Global App Configuration service (GACS).

For more information, see Automated sign-out on session disconnect.

ADMX file import support for Intune

Citrix Workspace app now supports the import of ADMX administrative template files in Microsoft Intune. This enhancement enables easier policy configuration and management for Workspace app deployments through Intune.

Modular Browser Content Redirection

Starting with the Citrix Workspace app 2507 for Windows, the Browser Content Redirection (BCR) component is now managed as a modular component, separate from the main Citrix Workspace app installer.

This new modular and evergreen model allows the Browser Content Redirection component to be updated independently and uninstalled independently. This feature provides the following key benefits:

- **Enhanced security**: The BCR Chromium Embedded Framework component can receive security patches and updates as soon as they are available, without waiting for a full Citrix Workspace app release.
- **Simplified Management**: Customers no longer need to update entire Citrix Workspace app to receive the latest Browser content redirection features.

- **Accelerated Innovation**: Faster deployment of new BCR features, enhancements, and bug fixes is now possible, delivering continuous value to customers

To ensure a consistent user experience, the Modular BCR component is installed by default in Citrix Workspace app.

> **Note:**
>
> In Citrix Workspace app 2402 LTSR, the BCR component was not installed by default. With Citrix Workspace app 2507 LTSR, BCR has undergone significant user experience improvements and is now installed by default.

> For more information, see Modular Browser Content Redirection.

Zoom 64-bit plug-in management support

Zoom has announced that Version 6.2.10 is the last version to support a 32-bit plugin. For more information, see Zoom documentation.

Starting from 2507 version onwards, Citrix Workspace app installs the Zoom plug-in management based on the endpoint architecture. If endpoint OS is 64-bit, then Citrix Workspace app installs 64-bit plugin management and keep it updated through auto-update service.

Simplified distribution of uberAgent on endpoints through Citrix Workspace app

uberAgent delivers advanced User Experience and Endpoint Security related insights. Starting with 2507 release, uberAgent is now packaged with Citrix Workspace app. This integration supports simplified distribution of uberAgent, streamlining deployment and reducing administrative overhead.

For more information, see uberAgent add-on support for managed devices in Citrix Workspace app.

Enhanced background blur persistence for webcam

Starting with version 2507, the background blur setting persists between sessions and reconnects. Citrix Workspace app remembers your preference automatically. You can enable the background blur feature by navigating to **Preferences** > **Connections** and select **Enable background blur**.

For more information, see Enhanced background blur persistence for webcam.

Enhanced keyboard layout settings notification

Starting with this release, the keyboard layout settings UI displays a warning that informs you that a session relaunch is required for changes to take effect.

For more information, see Enhanced keyboard layout settings notification.

Enable noise suppression

Starting with the 2507 version, Citrix Workspace app now offers improved audio redirection with enhanced noise suppression. This feature reduces background noise, ensuring clearer and more accurate speech, improving the overall communication experience.

Note:

This feature is disabled by default.

For more information, see Enable noise suppression.

Version upgrade for Chromium Embedded Framework

The version of the Chromium Embedded Framework (CEF) used in the Browser Content Redirection (BCR) is upgraded to **137**. This upgraded version includes fixes for known security vulnerabilities.

Citrix Enterprise Browser

This release includes Citrix Enterprise Browser version 139.1.1.18, based on Chromium version 139. For more information about the Citrix Enterprise Browser, see the Citrix Enterprise Browser documentation.

App Protection support for ARM64 on Windows

Starting with Citrix Workspace app for Windows version 2507, App Protection is supported on ARM64 devices running Citrix Workspace app in emulated mode. This update ensures that users on ARM64 machines can seamlessly use App Protection features. App Protection in this configuration can be leveraged to block screen capture attempts of sensitive content in protected applications by AI Agents like Microsoft Recall. For more information, see Blocking of Screen Capture from AI-Powered tools

Technical Previews

- Browser Profile Sharing in Browser Content Redirection
- HDX™ graphics superresolution upscaling

- Cross-session clipboard exchange

For the complete list of Technical Preview features, see the Features in Technical Preview page.

Feature included from previous releases

This release supports features that were included in Citrix Workspace app for Windows version from 2403 to 2503.10 as listed below.

2503.10

Audio Quality Enhancer to improve audio performance

Starting with version 2503.10, the audio quality enhancer is enabled by default for adaptive audio.

Audio quality enhancer maintains clear audio during brief network disruptions. This feature adapts to the network conditions to ensure consistent audio performance during playback and recording.

> **Note:**
>
> Both adaptive audio and loss tolerant mode for audio must be enabled for this feature to work.

Schedule automatic update using GACS

You can now define and schedule the timeframe in which the automatic Citrix Workspace app update must be performed using Global App Configuration Service (GACS).

- **Define timeframe for automatic update**: Administrators can now schedule automatic updates for Citrix products at any preferred time on their Windows devices. During this specified time, software updates automatically or users receive notifications on available updates.
- **Manage automatic update version and rollout period**: Administrators can schedule a convenient start date and rollout period for a specific version of Citrix Workspace app during which an automatic update is set to roll out to their end users. This capability allows them to determine the rollout dates, minimizing disruption to end users and improving the user experience.

For more information, see the Define timeframe for automatic update and manage automatic update version and rollout period for Citrix Workspace app documentation.

2503

The following features are added in this release:

- Client-side graphics optimizations
- Persistent session in Citrix Workspace app
- Enhanced Desktop Viewer toolbar
- Enhancement to connection strength indicator on Desktop Viewer toolbar
- Multi-monitor layout selection
- Enhancements on Desktop Lock or Boot to VDI feature
- Simplified SSON
- Seamless integration of deviceTRUST with Citrix Workspace app
- Enhancement to auto-update
- Enable auto-update for active users only
- Enhanced installation process for Citrix Workspace app with App Protection
- Improved installation process for Citrix Workspace app
- Auto-sync backend resource changes for Start menu and Desktop shortcuts
- Install Zoom and Webex plug-in managers during Citrix Workspace app installation
- Log collection support for non-admin users
- Enhanced security and compatibility with AppLocker
- Improved audio performance in Microsoft Teams
- Monitor third-party UC app optimization status using Citrix Director
- Hybrid launch support using GACS for on-premises stores
- Hybrid launch support using GACS for cloud stores - Technical Preview
- Browser Profile Sharing - Technical Preview
- Enable noise suppression - Technical Preview
- Screen recording for specific applications - Technical Preview

Client-side graphics optimizations

This release includes significant optimizations to the HDX client-side graphics engine, resulting in noticeable performance improvements and higher frame rates for a smoother user experience. For more information, see the Graphics section in the Citrix Virtual Apps and Desktops documentation.

Persistent session in Citrix Workspace app

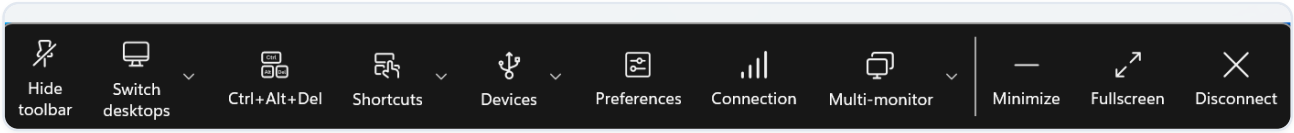
With this release, if you enable the Persistent session feature, Citrix Workspace app automatically detects session termination and relaunches the application or desktop without any user intervention when the application or desktop session logs out or disconnects.

This feature ensures uninterrupted application or desktop availability, improving user experience and productivity.

For more information, see Persistent Session in Citrix Workspace app documentation.

Enhanced Desktop Viewer toolbar

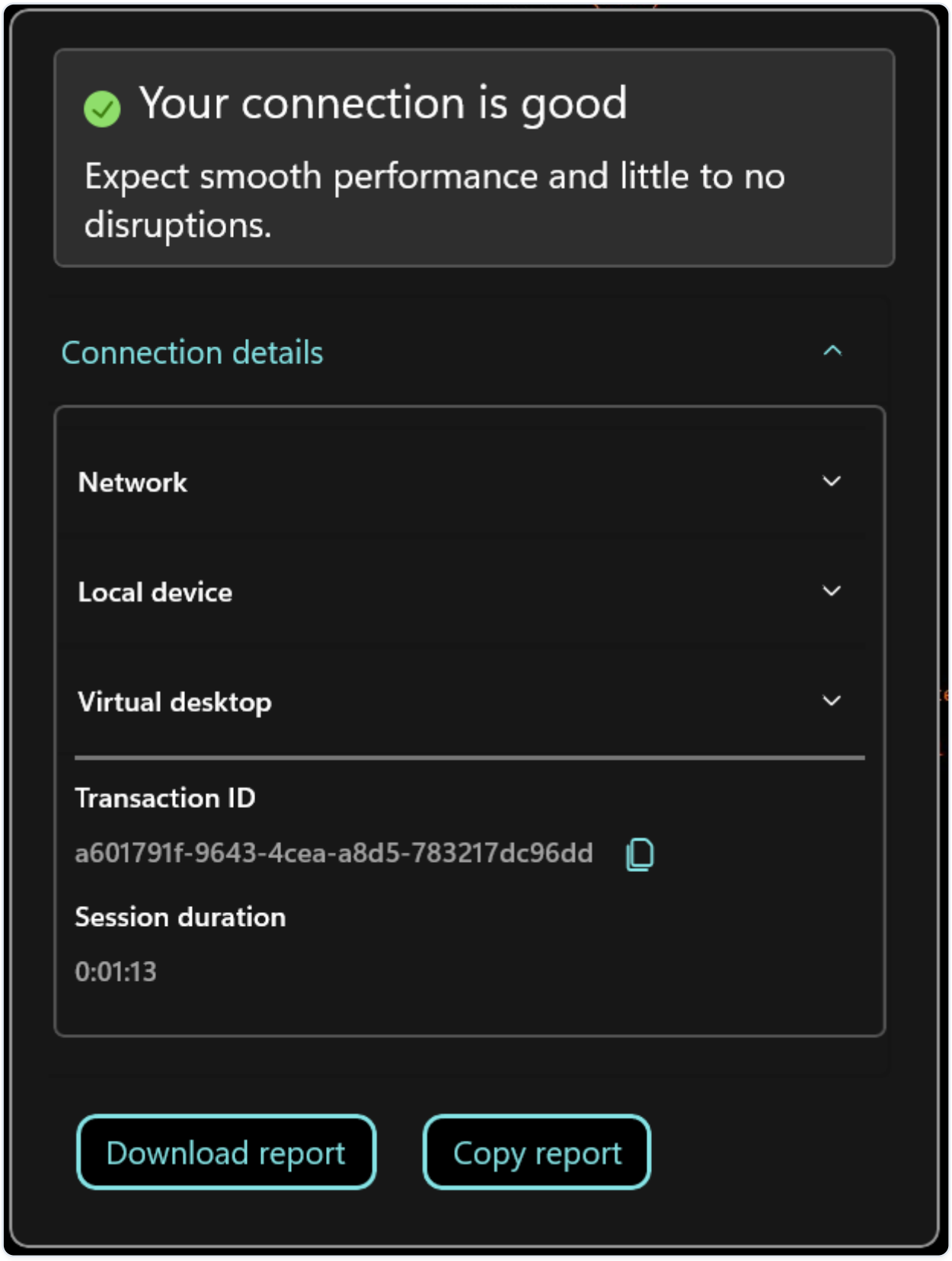
Starting with the 2503 version, Citrix Workspace app for Windows provides an enhanced Desktop Viewer toolbar.



For more information, see the Enhanced Desktop Viewer toolbar documentation.

Enhancement to connection strength indicator on Desktop Viewer toolbar

Starting with version 2503, the **Connection Strength Indicator** on the **Desktop Viewer** toolbar is enhanced with new features to provide a better user experience.



For more information, see the Enhancement to connection strength indicator on Desktop Viewer toolbar documentation.

Multi-monitor layout selection

Starting with version 2503, the **Multi-Monitor Selector (MMS)** allows users to choose which displays to use in full-screen mode for desktop sessions only, not for seamless sessions. A new **Multi-Monitor** button has been added to the toolbar, which appears only when more than one screen is connected. This feature enhances the flexibility and usability of multi-monitor setups in desktop sessions, providing a more tailored and efficient user experience.

For more information, see Multi-monitor layout selection documentation.

Enhancements on Desktop Lock or Boot to VDI feature

From this release, the Citrix Workspace app Desktop Lock, also known as the direct boot to VDI feature, includes the following enhancements:

- **Integrated Installer**: Desktop Lock is now part of the main Citrix Workspace app installer, simplifying deployment and distribution for admins. When you install Citrix Workspace app using:
  - **Command line installation**: You can enable Desktop Lock using command-line parameters during the installation.
  - **UI**: You can enable Desktop Lock using the Group Policy Object (GPO) policy after the installation.

  You need to reboot the machine after enabling the Desktop Lock feature.
- **De-coupled from SSON**: Previously, you had to install the Citrix Workspace app for Windows with the `/includeSSON` flag to enable the Desktop Lock feature. Desktop Lock is now available without single sign-on (SSON). However, it is recommended to use it with SSON enabled for a seamless experience.
- **Enable feature through policy or command line**: You can manage the feature enablement through GPOs. This enhancement provides granular controls to enable the feature at any point in time. The following policies can be managed in the Group Policy Editor:
  - **AllowDesktopLockOnMachine**: This policy is a machine-level policy that allows the ability to switch to Desktop Lock for any user on the machine. This requires a reboot of the machine.
  - **EnableDesktopLockforAllStandardUsers**: This policy is a machine-level policy that enables Desktop Lock for all standard users on the machine. Along with this policy, you need to enable the **AllowDesktopLockOnMachine** policy.

- **EnableDesktopLockforUser**: This policy is a user group policy to enable or disable Desktop Lock for a specific user. Along with this policy, you need to enable the **AllowDesktopLockOnMachine** policy.

-. **Post-installation configuration**: Stores can be configured post-installation, extending Desktop Lock to existing stores configured through GPO.

- **Support for any identity provider (IDP)**: Desktop Lock now supports booting into VDI with any IdP that supports Citrix Workspace app.

> **Note:**
>
> You must reboot the machine after upgrading Citrix Workspace app for Windows with the Desktop Lock feature for the changes to take effect.

> For more information, see the Citrix Workspace app Desktop Lock documentation.

Simplified SSON

Previously, to enable the single sign-on (SSON) feature, you had to install the Citrix Workspace app for Windows with the `/includeSSON` flag or select the **Enable Single Sign-on** checkbox during installation.

With this release, the system installs SSON by default in dormant mode. You can enable SSON post-installation using the Group Policy Object (GPO) policy. To enable, navigate to **User Authentication > Local user name and password** and select the **Enable pass-through authentication** checkbox.

> **Note:**
>
> You must reboot the system after updating the GPO policy for the setting to take effect.

Seamless integration of deviceTRUST with Citrix Workspace app

Starting with version 2503, Citrix Workspace app for Windows includes deviceTRUST, enhancing security through continuous device posture checks within the session. deviceTRUST is packaged with Citrix Workspace app for unified deployment, ensuring seamless integration and management.

For more information, see the Seamless integration of deviceTRUST with Citrix Workspace app for Windows.

Enhancement to auto-update

The auto-update of Citrix Workspace app is now enhanced with the following features:

- **Define timeframe for automatic update**: Administrators can now schedule automatic updates for Citrix products at any preferred time on their Windows devices. During this specified time, software updates automatically or users receive notifications on available updates.
- **Manage automatic update version and rollout period**: Administrators can schedule a convenient start date and rollout period for a specific version of Citrix Workspace app during which an automatic update is set to roll out to their end users. This capability allows them to determine the rollout dates, minimizing disruption to end users and improving the user experience.

You can enable these features using Group Policy Object (GPO).

Benefits:

- **Custom rollout period**: Admins can determine the rollout period for their organization, overriding the default period set by Citrix.
- **Scheduled updates**: Admins can specify the hours or time frame during the day to check for and update Citrix Workspace app.
- **Flexible update days**: Admins can choose a specific start date to specify when to download and begin installation updates.

For more information, see the Define timeframe for automatic update and manage automatic update version and rollout period for Citrix Workspace app documentation.

Enable auto-update for active users only

Starting with version 2503, the auto-update feature has been enhanced to trigger only for active users.

For more information, see the Enabled auto-update for active users only documentation.

Enhanced installation process for Citrix Workspace app with App Protection

Previously, when App Protection was enabled, the `/cleanInstall` switch was not supported, and the user had to manually uninstall and reboot the machine before retrying installation. Starting with version 2503, when App Protection is enabled and when running the `/cleanInstall`

command, Citrix Workspace app automatically uninstalls, reboots the machine based on user selection, and reinstalls the app during the reboot.

For more information, see the Enhanced installation process for Citrix Workspace app with App Protection documentation.

Improved installation process for Citrix Workspace app

Citrix Workspace app installation is now more robust. In version 2503, the installer is improved to handle situations where other installations (like Windows Update) are in progress. Instead of failing, Citrix Workspace app now waits for the other installation to complete, ensuring a successful installation.

Auto-sync backend resource changes for Start menu and Desktop shortcuts

The auto-sync backend resource changes feature enhances the user experience by automatically synchronizing backend resource changes for the start menu and desktop shortcuts.

Key features:

- **Updating shortcuts with updated resource path**:

  The shortcut automatically points to the new path when the resource path is updated in the backend, eliminating the need for manual refresh. This feature is enabled by default.

- **Option to show disabled shortcuts**:

  The shortcut remains visible even when a resource is disabled in the backend. Previously, the shortcut was removed when a resource was disabled. This feature is useful for temporary maintenance, allowing users to retain the shortcut. This feature is disabled by default and can be enabled using the **Show Disabled Shortcut** setting in either the Global App Configuration Service (GACS) or the Group Policy Object template.

For more information, see the Auto-sync backend resource changes for Start menu and desktop shortcuts documentation.

Install Zoom and Webex plug-in managers during Citrix Workspace app installation

Citrix Workspace app version 2503 provides an option to install the Zoom and Webex plug-in managers during the installation. You can use either the UI or command-line for this installation.

For more information, see the Install plug-ins documentation.

Log collection support for non-admin users

This feature extends the Citrix Workspace app for Windows log collection capability to support non-admin users. Previously, log collection was partially supported for users for whom Citrix Workspace app was installed by an admin. With this enhancement, complete log collection is now possible for users for whom Citrix Workspace app is installed by an admin.

Enhanced security and compatibility with AppLocker

Citrix Workspace app for Windows now offers improved compatibility with AppLocker, a security posture tool. This enhancement addresses security concerns and enhances the user experience by aligning more effectively with AppLocker policies.

With this release, application stubs created using File Type Association (FTA) are no longer created by default. Previously, these stubs were unsigned binaries, and AppLocker settings were often required to block them from running. By eliminating the creation of unsigned application stubs, this feature strengthens security and minimizes potential vulnerabilities in environments configured with AppLocker.

Improved audio performance in Microsoft Teams

Starting with the Citrix Workspace app for Windows version 2503, the audio subsystem used in the **HDXRTCMediaEngine** has been replaced with a newer system. As a result, Microsoft Teams now provides better audio performance, enhancing the overall user experience during calls and meetings. Along with this feature, the following issues related to Microsoft Teams optimization have been resolved:

- The new plug-in device might not be available in the **Microphone** drop-down menu option.
- Duplicate entries of devices might be present in the **Microphone** drop-down menu option.
- Users might not hear from the new plug-in headset when the default output devices (**Speakers/ Headphones**) on the client are disabled.
- Unplugging the last connected device might make the system unresponsive.

Monitor third-party UC app optimization status using Citrix Director

You can now monitor details about third-party Unified Communications (UC) applications and their plug-ins using **Citrix Director**. This feature helps administrators monitor performance and troubleshoot issues, ensuring a consistently positive user experience.

PREREQUISITES

- Virtual Delivery Agent (VDA) 2503

For more information, see the Director documentation.

BENEFITS

- **Enhanced visibility**: A unified view of UC app optimization status in Director simplifies monitoring and troubleshooting across multiple vendors.
- **Improved user experience**: Proactive issue identification and resolution ensure optimal collaboration experiences for end-users.
- **Streamlined IT operations**: Centralized monitoring reduces complexity and empowers administrators to efficiently manage UC environments.

This feature enables active issue resolution and ensures a consistently positive user experience.

Hybrid launch support using GACS for on-premises stores

Starting with version 2503, Citrix Workspace app for Windows supports management using Global App Configuration Service (GACS) in hybrid launch for on-premises stores. In a hybrid launch scenario, users access Citrix resources through a web browser. When an application or desktop is selected, Citrix StoreFront™ generates an ICA file with the necessary launch instructions. The locally installed Citrix Workspace app then reads the ICA file, and establishes a secure connection to the remote application or desktop.

For more information, see Hybrid launch support using GACS for on-premises stores.

Technical Previews

- Hybrid launch support using GACS for cloud stores
- Browser Profile Sharing
- Enable noise suppression
- Screen recording for specific applications

For the complete list of Technical Preview features, see the Features in Technical Preview page.

2409.10

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

2409.1

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

2409

> **Note:**

- The minimum required version of .NET Desktop Runtime is 8 for Citrix Workspace app for Windows 2409.

The following features are added in this release:

- Support for Windows 11 24H2
- Feature flag management
- Single sign-on support for Edge WebView when using Microsoft Entra ID
- Enhanced virtual desktop screen resizing experience
- Enhanced desktop launch experience
- Enhancement to sustainability initiative
- Streamlined beacon checks
- .NET requirements
- SOCKS5 proxy support for EDT
- Customization of Desktop Viewer toolbar
- Remember USB connections
- Disabling the “Exiting Full Screen Mode” tip prompt
- Support for WebHID API in UCSDK
- Support for TLS protocol version 1.3
- Disabling TLS 1.0 or 1.1 communication protocols
- Default audio device selection
- Connection Strength Indicator on Desktop Viewer toolbar
- Enable Audio Quality Enhancer to improve audio performance (Technical Preview)
- Virtual Channel Plugin Manager
- Deprecation of PNAgent-based stores

Support for Windows 11 24H2

Citrix Workspace app for Windows 2409 provides support for the Windows 11 24H2 release. This ensures a smooth transition for users upgrading to the latest Windows version and allows them to continue using Citrix Workspace app without any disruption.

Note:

> The **Enable MPR notifications for the System** policy in the Group Policy Object template must be enabled to support the domain pass-through (single sign-on) authentication feature on Windows 11. By default, this policy is disabled on Windows 11 24H2. So, if upgraded to Windows 11 24H2, you must enable the **Enable MPR notifications for the System** policy.

Feature flag management

Citrix is changing the way that it manages feature flags, allowing access to preview features and enabling dynamic management of features in production. To ensure optimal functioning of features that are under feature flags, you need to enable traffic to the URL `features.netscalergateway.net`.

For more information, see Feature flag management.

Single sign-on support for Edge WebView when using Microsoft Entra ID

Previously, when using Entra ID, authentication failed for Citrix Workspace app. With this release, Citrix Workspace app supports single sign-on (SSO) for Edge WebView when using Entra ID for authentication.

You can enable this feature using the UI or through Group Policy Object (GPO).

For more information, see Single sign-on support for Edge WebView when using Microsoft Entra ID.

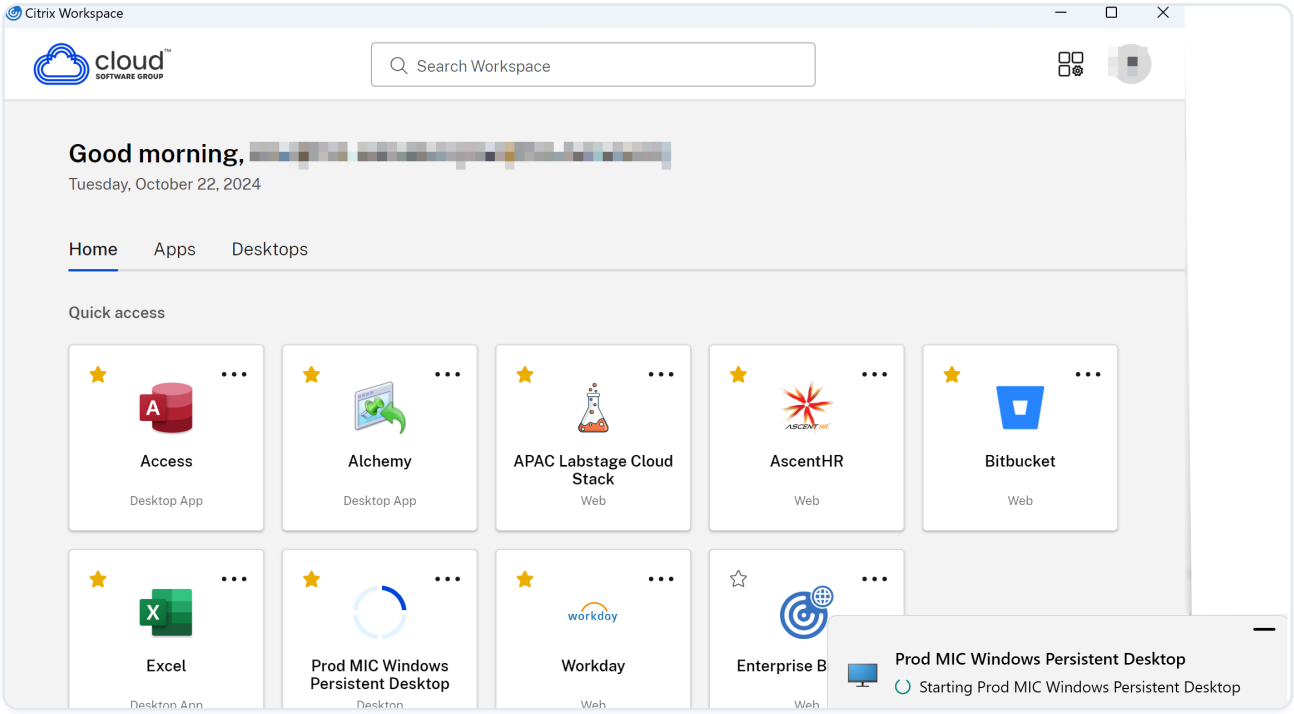
Enhanced virtual desktop screen resizing experience

Starting with the 2409 version, Citrix Workspace app for Windows ensures a smooth transition and prevents dark screens and flickers when resizing or stretching your virtual desktop screen. This feature is enabled by default.

For more information, see Enhanced virtual desktop screen resizing experience.

Enhanced desktop launch experience

Starting with version 2409, Citrix Workspace app for Windows ensures an enhanced desktop launch experience. You experience a seamless, flicker-free transition to your desktop without intermediate screens. The app also eliminates dark screens and flickering during resizing or stretching, providing a stable and modern interface. This feature is enabled by default.



For more information, see Enhanced desktop launch experience.

Enhancement to sustainability initiative

With this release, the sustainability initiative from Citrix Workspace app is enhanced to include the following extra keywords:

- `ICA-Title="sample title"`: The sample title is shown as the title. It's recommended to limit the title character count to 30.
- `ICA-Icon=true`: The green-leaf icon is shown. If set to false, the green leaf icon is hidden.

Example:

```
KEYWORDS: ICA-LogOffOnClose=true ICA-PromptMessage="Do you want to sign out from the session?" ICA-Title="Logout or disconnect" ICA-Icon=true
```

Note:

With this enhancement, if old keywords are detected, the behavior reverts to the default behavior.

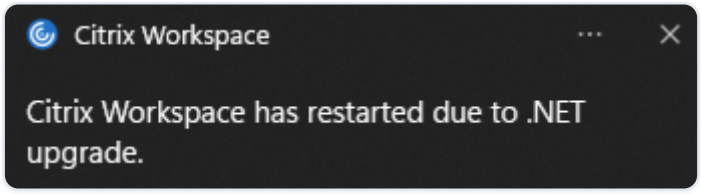
For more information, see the Sustainability initiative from Citrix Workspace app section.

Streamlined beacon checks

With this release, you can now use a single internal beacon to determine the network location, eliminating the need for both external and internal beacons. This feature reduces dependencies, enhances reliability, and improves the end-user experience.

.NET requirements

Citrix Workspace app for Windows now requires .NET Desktop Runtime 8.0 (8.0.4 or later). If the endpoint updates the .NET Desktop Runtime, any .NET Core-based app running at the time of the update might exhibit inconsistent behavior. To mitigate this issue, Citrix Workspace app restarts itself. Users receive the following notification once the restart is complete:



Any active sessions continue to work.

For endpoints with .NET 8.0.10 or later, see Knowledge Center article CTX692228.

For more information see, .NET requirements.

SOCKS5 proxy support for EDT

Previously, Citrix Workspace app only supported HTTP proxies operating on TCP. However, SOCKS5 proxy functionality was already fully supported within the Virtual Delivery Agent (VDA). For more information on VDA support, see the Rendezvous V2 documentation.

With this release, Citrix Workspace app now supports SOCKS5 proxies for Enlightened Data Transport (EDT), enhancing compatibility with modern enterprise network configurations.

Key benefits:

- Expanded proxy compatibility: Connect seamlessly through SOCKS5 proxies, widely used by enterprise networking teams for their support of both TCP and UDP traffic.
- Improved EDT performance: Use the full benefits of EDT (UDP-based) for optimized data transfer within Citrix Workspace app sessions.

For more information see, SOCKS5 proxy support for EDT.

Customization of Desktop Viewer toolbar

With this release, you can customize the options on the **Desktop Viewer** toolbar using the Global App Configuration service, Group Policy Editor, or any third-party endpoint management software capable of pushing Windows registry keys.

For more information see, Customization of Desktop Viewer toolbar,

Remember USB connections

This feature enhances the user experience when remoting USB devices to a Citrix Virtual Apps and Desktops™ session. While auto-redirection supports using device rules exists, this feature simplifies the process by remembering manually requested connections and reconnecting them with minimal configuration.

For more information see, Remember USB connections.

Disabling the "Exiting Full Screen Mode" tip prompt

Starting with Citrix Workspace app for Windows 2409, you can suppress the "Exiting Full Screen Mode" tip prompt that appears during HDX sessions using the Registry Editor.

For more information see, Disabling the “Exiting Full Screen Mode” tip prompt.

Support for WebHID API in UCSDK

Starting with the 2409 version, Citrix Workspace app for Windows supports the WebHID API to redirect Human Interface Device (HID) from an endpoint to Unified Communication SDK (UCSDK) integrated app on the VDI. It complies with the HID standard for bi-directional communication between the app that is integrated with UCSDK and the HID devices connected to the endpoint. With this feature, your UCSDK app interprets the **HID headset** commands such as Call accept, reject, mute, or unmute and so on in the HDX session for an enhanced user experience. This feature is enabled by default.

For more information see, Support for WebHID API in UCSDK.

Support for TLS protocol version 1.3

Starting with this release, Citrix Workspace app supports the Transport Layer Security protocol (TLS) version 1.3.

> **Note:**
>
> This enhancement requires VDA version 2303 or later.

> This feature is disabled by default.

For more information, see Support for TLS protocol version 1.3.

Disabling TLS 1.0 or 1.1 communication protocols

Starting with Citrix Workspace app for Windows 2409, the use of TLS 1.0 or 1.1 communication protocols is no longer enabled nor supported by default. This change enhances security by removing deprecated and potentially insecure protocols.

Benefits:

- Enhanced Security: Disabling outdated protocols reduces the risk of security vulnerabilities.
- Compliance: Aligns with industry standards and recommendations, such as RFC 8996.

Default audio device selection

Starting with the 2409 version of Citrix Workspace app, you can now select your preferred audio devices directly from the **Preferences** section. This feature allows for the splitting of audio devices across different VDA (VDAs) and monitors, providing a more customized audio experience.

For more information, see Default audio device selection.

Virtual Channel Plugin Manager

The Virtual Channel Plugin Manager can detect when the end-user on the VDA launches a third-party application (for example, New Microsoft Teams), check if its respective VDI plug-in is already installed on the endpoint, and prompt the user to install the plug-in if it is not.

For more information, see the Virtual Channel Plugin Manager documentation.

Connection Strength Indicator on Desktop Viewer toolbar

Starting with version 2409, Citrix Workspace app for Windows now supports the Connection Strength Indicator (CSI) on the **Desktop Viewer** toolbar. This feature displays a network strength icon that alerts you of network issues. You can click the indicator to view real-time connection statistics for the client and VDA, and copy diagnostic information to share with IT for advanced troubleshooting.

Benefits:

- Immediate feedback: The network strength icon gently nudges users when network issues are detected.
- Enhanced troubleshooting: Real-time stats and diagnostics help users and IT teams quickly identify and resolve connectivity issues.

For more information, see the Connection Strength Indicator on Desktop Viewer toolbar.

Deprecation of PNAgent-based stores

Starting from the 2409 release, PNAgent-based stores are no longer supported. PNAgent support was officially deprecated in the 2403 release. For more information, see the Deprecation table.

> **Note:**
>
> We recommend connecting through StoreFront using a store URL instead.

Citrix Enterprise Browser

This release includes Citrix Enterprise Browser version 130.1.1.12, based on Chromium version 128. For more information about the Citrix Enterprise Browser, see the Citrix Enterprise Browser documentation.

Technical Previews in 2409

- Enable Audio Quality Enhancer to improve audio performance

For the complete list of Technical Preview features, see the Features in Technical Preview page.

2405.11

> **Note:**
>
> The **Enable MPR notifications for the System** policy in the Group Policy Object template must be enabled to support the domain pass-through (single sign-on) authentication feature on Windows 11. By default, this policy is disabled on Windows 11 24H2. So, if upgraded to Windows 11 24H2, you must enable the **Enable MPR notifications for the System** policy.

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

2405.10

> **Note:**

> The minimum Microsoft Visual C++ Redistributable version required for Citrix Workspace app for Windows 2405.10 is 14.40.33810.0.

> This release addresses issues that help to improve overall performance, security, and stability.

2405

The following features are added in this release:

- Compatibility with the higher versions of .NET
- Single sign-on support for ARM64-based devices
- New Add-ons and packaging
- Configure store names for your store URL
- Improved Beacon checker tool
- Option to prevent endpoint from going to sleep when a session is active
- Enhancement to relative mouse
- Share system audio
- Upgraded version of WebRTC for the optimized Microsoft Teams
- Support for MJPEG webcams
- Enhanced System Logs for browser content redirection
- Browser Content Redirection and Microsoft Teams Optimization support for ARM64 based devices[Technical Preview]
- App Protection support for double-hop scenario
- Citrix Enterprise Browser
    - Modify the user-agent of Citrix Enterprise Browser
    - Additional security restrictions for the Citrix Enterprise Browser

Compatibility with the higher versions of .NET

Citrix Workspace app for Windows version 2405 is compatible with the higher versions of .NET that are supported on your system. To ensure this compatibility, Citrix Workspace app follows these installation rules:

- If .NET 6.0.20 or any supported higher version of .NET is installed on the system, Citrix Workspace app does not install any additional .NET versions.

- If.NET isn't installed on the system or a version less than 6.0.20 is installed on the system, Citrix Workspace app installs .NET version 6.0.25.
- If you install any supported higher version of .NET, Citrix Workspace app is compatible with the highest available .NET version. For example, you can install .NET 8.x and uninstall .NET 6.0.25. In this case, Citrix Workspace app uses the .NET 8.x version.

Single sign-on support for ARM64-based devices

From this 2405 release, Citrix Workspace app for Windows supports the single sign-on feature on the ARM64-based devices. For more information on single sign-on, see the Authentication page.

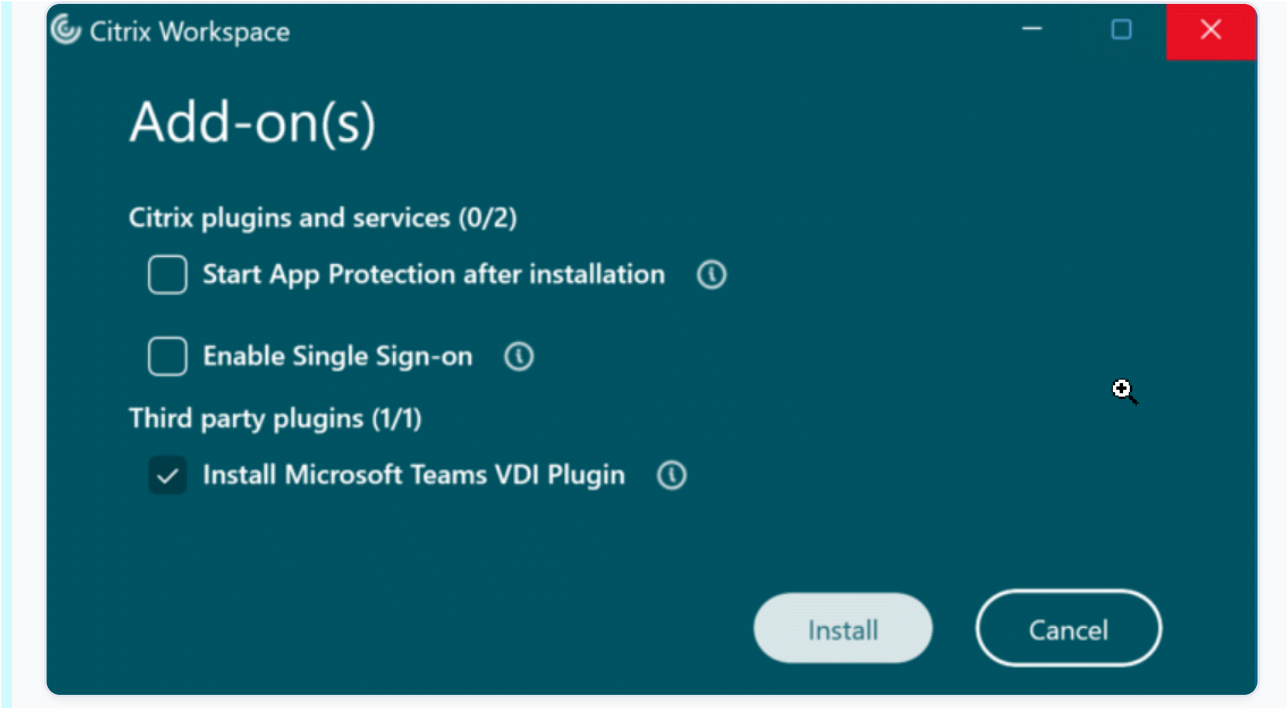
New Add-ons and packaging

From Citrix Workspace app for Windows 2405 version, you can choose the following from the **Add-on(s)** page during the upgrade of Citrix Workspace app:

- Start App Protection after installation
- Enable single sign-on
- Install Microsoft Teams VDI Plugin

You can uninstall the Microsoft Teams Optimization VDI plug-in independent of Citrix Workspace app.

> **Note:**
>
> If a plug-in is already installed on your system, that plug-in option is selected automatically for upgrade. Also, if you don't have sufficient privileges to download the plug-in, that option won't be visible on the **Add-on(s)** page.



Configure store names for your store URL

With this feature, admins can give the stores a user friendly name to recognize. In addition, admins can enable or disable the ability for end users to modify the store name on their Citrix Workspace app.

For more information, see Configure store names for your store URL.

Improved Beacon checker tool

As part of the Configuration Checker utility, Citrix Workspace app allows you to do a beacon test using the Beacon checker tool.

Earlier the Beacon test supported only the `ping.citrix.com` beacon. Starting from Citrix Workspace app for Windows 2405 version onwards, beacon test works for all the beacons configured in the store added in Citrix Workspace app.

For more information, see Configuration Checker and Beacon test.

Option to prevent endpoint from going to sleep when a session is active

When a user with an active session stays away from the virtual desktop without any mouse or keyboard activity, the endpoint device might go into sleep mode after completing the set time for Windows sleep mode. As a result, the Citrix session might be disconnected and when the user returns to the session, the user might be unable to reconnect to the existing session.

With this release, a new policy named Power Management is introduced to prevent the endpoint devices from going to sleep when a session is active.

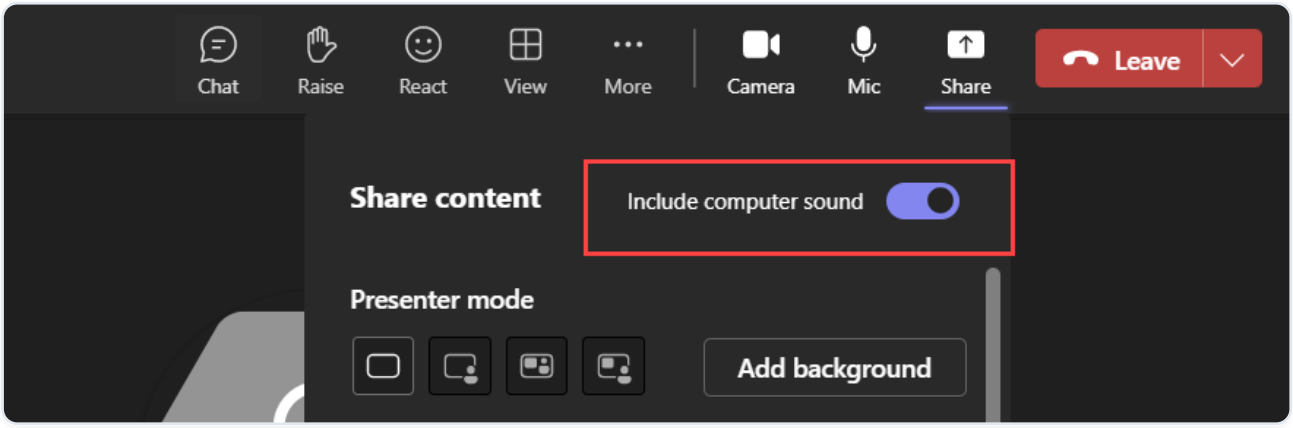
For more information, see Option to prevent endpoint from going to sleep when a session is active.

Enhancement to relative mouse

With this release you can restrict the usage of the mouse to the window using the preferences UI available from the toolbar. This enhancement helps you to use the apps that need to monitor mouse movement extending to or beyond the boundaries of the virtual desktop's screen. These apps include third-party apps or those apps that scroll a view in response to mouse movement. For more information, see Enhancement to relative mouse.

Share system audio

You can now share the audio playing on your VDA with participants in a meeting. Select the **Include computer sound** option to make your meetings more engaging. This feature is enabled by default. For end users, to use the feature, turn on **Include computer sound** on before sharing their screen.



Limitations:

- Audio cannot be shared using this feature when sharing the screen with RAVE and BCR redirected apps or tabs.
- This feature is supported only on published desktops.

Upgraded version of WebRTC for the optimized Microsoft Teams

The version of WebRTC that is used for the optimized Microsoft Teams is upgraded.

Support for MJPEG webcams

Starting with the 2405 version, MJPEG webcams are supported in the H264 stream. The webcam performs MJPEG compression internally which provides better image quality and a higher frame rate.

This feature is enabled by default. However, if certain Webcam doesn't support MJPEG, this feature is disabled.

Enhanced System Logs for browser content redirection

With the enhancements to the System Logs, browser content redirection now allows admins to monitor the feature status. For more information, see Browser content redirection.

App Protection support for double-hop scenario

Starting with the Citrix Workspace app for Windows 2405 version, App Protection is supported for the double-hop scenario when installed on a workstation VDA (such as Windows 10 or Windows 11) for a single-session VDA.

The following features are currently supported:

- Anti-keylogging
- Anti-screen capture

For more information, see App Protection with double-hop scenario.

MODIFY THE USER-AGENT OF CITRIX ENTERPRISE BROWSER

Administrators can now modify the Citrix Enterprise Browser's user-agent for any internal web or SaaS apps. You can configure this through Global App Configuration service. This feature provides the flexibility to create different variations of the user-agent for Citrix Enterprise Browser, which you can use for various uses.

One such use-case is the ability to restrict the internal web or SaaS apps to open only in Citrix Enterprise Browser. In addition to modifying the user-agent, you need to configure the Identity Provider (IdP) to perform a conditional check that verifies whether the end user is trying to open the app using Citrix Enterprise Browser or a native browser. The IdP opens the app only if end user tries to access it using Citrix Enterprise Browser. This restriction prevents users from accessing sensitive information in these apps from other browsers.

For more information, see Use Case 3c - Restrict apps to Citrix Enterprise Browser by modifying its user-agent.

ADDITIONAL SECURITY RESTRICTIONS FOR THE CITRIX ENTERPRISE BROWSER

Citrix introduces additional access restrictions to enhance the security and user experience of Citrix Enterprise Browser with Secure Private Access and Global App Configuration service (GACS).
Restrictions managed through Secure Private Access
Copy:

Administrators can enable or disable copying of data from a SaaS or internal web app with this access policy when accessed using Citrix Enterprise Browser. The default value is Enabled.

For more information, see the Copy restriction in the Secure Private Access product documentation.

Paste:

Administrators can enable or disable pasting of copied data into the SaaS or internal web app with this access policy when accessed using Citrix Enterprise Browser. The default value is Enabled.

For more information, see the Paste restriction in the Secure Private Access product documentation.

Personal data masking:

Administrators can use the **Personal data masking** restriction to mask various types of sensitive information such as credit card numbers, social security numbers, and dates. Also, you have the flexibility to define custom rules for detecting specific types of sensitive information and masking it accordingly. The **Personal data masking** restriction has the option to fully or partially mask the information.

For more information, see Personal data masking.

Upload restriction by file type:

Administrators can restrict file uploads based on MIME (multi-purpose internet mail extensions) types. Unlike the **Uploads** policy, which allows you to enable or disable all file uploads, the **Upload restriction by file type** restriction allows you to enable or disable file uploads for specific MIME types.

For more information, see Upload restriction by file type.

Download restriction by file type:

Administrators can restrict file downloads based on MIME (multi-purpose internet mail extensions) types. Unlike the **Downloads** policy, which allows you to enable or disable all file downloads, the **Download restriction by file type** restriction allows you to enable or disable file downloads for specific MIME types.

For more information, see Download restriction by file type.

Printer management:

Enterprises can now prevent the printing of confidential documents and unauthorized data sharing. Admins can configure this policy through Secure Private Access. Admins can configure the behavior for network printers, local printers, and print using the **Save as PDF** option.

The following options are available for administrators to control access to printers for the end users:

- **Network printers:** A network printer is a printer that can be connected to a network and used by multiple users.
    - **Disabled:** Printing from any network printers in the network is disabled.
    - **Enabled:** Printing from all network printers is enabled. If printer host names are specified, then all other network printers apart from the ones specified are blocked.

> **Note:**
>
> Printers are identified by their host names.

- **Local printers:** A local printer is a device directly connected to an individual computer. This connection is typically facilitated through Bluetooth, USB, parallel ports, or other direct interfaces.
    - **Disabled:** Printing from all local printers is disabled.
    - **Enabled:** Printing from all local printers is enabled.
- **Print using Save as PDF**
    - **Disabled:** The Save as PDF option for saving the content in PDF format is disabled.
    - **Enabled:** The Save as PDF option for saving the content in PDF format is enabled.

> **Note:**
>
> - If the admin has disabled certain printing options, then those options appear grayed out to the end users.
> - End users can't use the network printer if it is renamed on their device.

> **Clipboard restriction for Security groups:**

In Secure Private Access, administrators can restrict clipboard access to any designated group of apps. These designated groups of apps are created as **Security groups** in Secure Private Access, so that the end users are permitted to copy and paste contents only within that Security groups. There is also an Advanced option to enable copy and paste contents between Security groups and other local apps on the machines or unpublished web apps.

For more information, see Clipboard restriction for Security groups.
Restrictions managed through the Global App Configuration service
Clipboard restriction:

In GACS, administrators can use the **Enabled Sandboxed Clipboard** option to manage clipboard access. When you restrict clipboard access through GACS, all content copied from any website accessed within the Citrix Enterprise Browser can't be pasted outside the Enterprise Browser. Similarly, any content copied from native apps can't be pasted into any website accessed within the Enterprise Browser.

For more information, see Clipboard restriction.

Audio Capture Allowed:

Administrators can use this setting to enable or disable audio capture access. When an administrator enables this setting, or leaves it unset, users are prompted to allow audio capture access. When an administrator disables this setting, these prompts are turned off, and audio capture is blocked.

For more information, see Audio Capture Allowed.

Video Capture Allowed:

Administrators can use this setting to enable or disable video capture access. When an administrator enables this setting, or leaves it unset, users are prompted to allow video capture access. When an administrator disables this setting, these prompts are turned off, and video capture is blocked.

For more information, see Video Capture Allowed.

Technical Preview

- Browser Content Redirection and Microsoft Teams Optimization support for ARM64-based devices

For the complete list of Technical Preview features, see the Features in Technical Preview page.

2403.1

This release addresses issues that help to improve overall performance, security, and stability.

2403

The following features are added in this release:

- Sustainability initiative for cloud hybrid launch
- Enhanced domain pass-through for single sign-on (Enhanced SSO)
- Support for advanced NetScaler policies for Storebrowse on Windows
- Install Microsoft Teams VDI plug-in for Citrix
- Hide Troubleshooting and Send Feedback options for end users
- Deprecation of PNAgent support
- App Protection
  - Screen Capture Allow List
  - Process exclusion list
  - USB Filter Driver Exclusion List
- Citrix Endpoint Analysis
- Citrix Enterprise Browser
  - Security indicator when visiting websites
  - (#Citrix Enterprise Browser introduces additional settings in the Global App Configuration service)

Sustainability initiative for cloud hybrid launch

> **Note:**

> This feature was previously available for native launches (cloud and on-premises) from the Citrix Workspace app 2309 version onwards.

> From the Citrix Workspace app 2403 version, this feature is available for hybrid launches on cloud. After this feature is enabled, a prompt appears to sign out from the desktop session when a user closes a virtual desktop. This feature helps conserve energy if there are Windows OS policies that are used to shut down VMs when no users are logged in. You can

> also customize the text that appears on the **Save energy** screen. For more information, see Sustainability initiative for cloud hybrid launch.

Enhanced domain pass-through for single sign-on (Enhanced SSO)

Previously, Citrix Workspace app for Windows supported only SSON or domain pass-through authentication for single sign-on to Citrix Virtual Apps and Desktops environments using user credentials. This authentication enables the user to authenticate to the domain on their device and use their virtual apps and desktops without having to reauthenticate again.

With this release, Citrix Workspace app supports enhanced domain pass-through which is a new method of SSO. It uses Kerberos authentication instead of user credentials. Users can now sign in to Citrix Virtual Apps and Desktops and to StoreFront using integrated windows authentication. For more information, see Enhanced domain pass-through for single sign-on (Enhanced SSO).

Support for advanced NetScaler policies for Storebrowse on Windows

Citrix Workspace app for Windows now supports advanced policies on NetScaler Gateway with Storebrowse. The supported authentication protocol is LDAP authentication. Storebrowse is a command-line utility that interacts between the client and the server. It's used to authenticate all the operations within StoreFront and with Citrix Gateway. For more information, see the Storebrowse page.

> **Note:**

> The nFactor authentication protocol isn't supported with Storebrowse on Windows.

Install Microsoft Teams VDI plug-in for Citrix

You can now install the Microsoft Teams VDI plug-in during the installation of Citrix Workspace app using one of the following options.

- Using UI
- Using command-line

> **Note:**

> For version compatibility with VDI and configuration details, see Microsoft Teams 2.1 supported for VDI/DaaS and New Microsoft Teams VDI requirements.

Hide Troubleshooting and Send Feedback options for end users

Admins can now hide the troubleshooting and send feedback options for their end users using the GPO editor. Once this setting is enabled, the **Troubleshooting** and **Send Feedback** options which were previously visible to the end users on the system tray is hidden. For more information, see Hide Troubleshooting and Send Feedback options for end users.

App Protection

SCREEN CAPTURE ALLOW LIST

If Citrix Workspace app, virtual apps and desktops, or SaaS apps are enabled with the App Protection Anti-screen capture policy, then you can't capture their screens using any screen-capturing tool.

However, starting from the Citrix Workspace app for Windows 2403 release, the Screen Capture Allow List feature enables you to add an app to the screen capture allow list. This feature enables you to use the allow listed app and capture the screen of the resource enabled with the App Protection Anti-screen capture policy. For more information, see Screen Capture Allow List.

PROCESS EXCLUSION LIST

When you launch any process or application on your device, App Protection DLLs are injected into each process if the App Protection is enabled. Sometimes, this might cause the process or application not to work due to compatibility issues with the DLL.

Starting from the Citrix Workspace app for Windows 2403 release, you can add any process to the Process exclusion list to avoid the injection of the App Protection DLL into that particular process and recover from any compatibility issues caused by the presence of App Protection DLLs. For more information, see Process exclusion list.

USB FILTER DRIVER EXCLUSION LIST

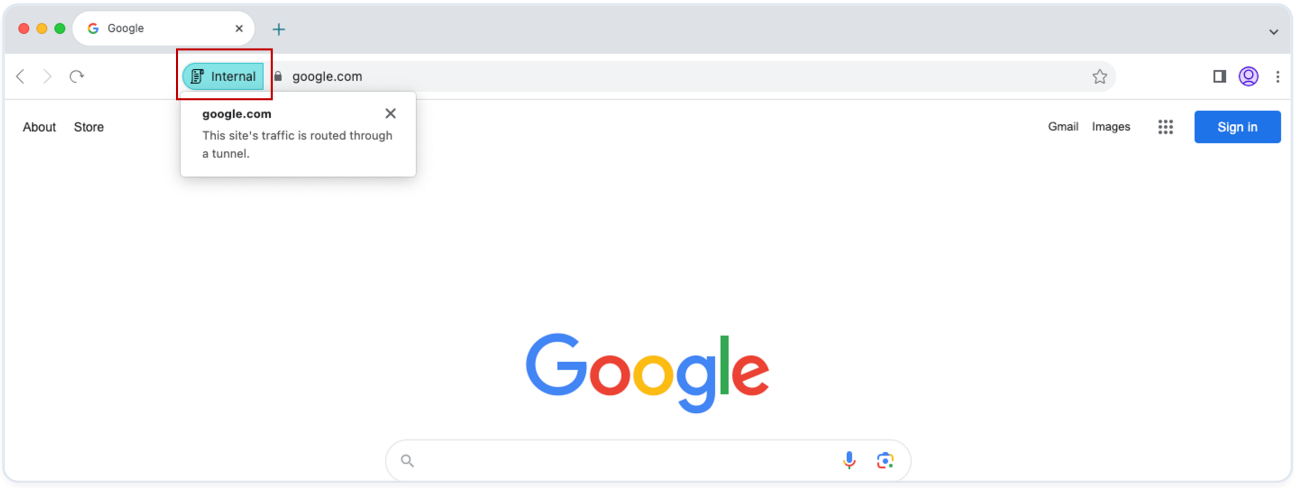
Sometimes, when you're using specialized external keyboards such as gaming keyboards with the Citrix Workspace app, the App Protection USB Filter Driver might cause compatibility issues and block you from using the keyboard.

Starting from the Citrix Workspace app for Windows 2403 release, the USB Filter Driver Exclusion List feature allows you to exclude any USB device that has compatibility issues with the Citrix Workspace app using the device Vendor ID and Product ID. For more information, see USB Filter Driver Exclusion List.

SECURITY INDICATOR WHEN VISITING WEBSITES

Citrix Enterprise Browser now displays a security indicator on the address bar when users visit any websites. The indicator aims to inform users about the security aspects of the websites, such as whether it's an internal site or if there are any potential security restrictions. The indicator provides more information when you click it. The indicator appears on the Enterprise browser by default, and it enhances the user experience.





CITRIX ENTERPRISE BROWSER INTRODUCES MORE SETTINGS IN THE GLOBAL APP CONFIGURATION SERVICE

More settings have been added into the Global App Configuration service (GACS) for configuring Citrix Enterprise Browser.

- Enable autofill address - Allows administrators to enable or disable the autofill suggestions for addresses.
- Enable autofill credit card - Allows administrators to enable or disable the autofill suggestions for credit card information.
- Auto launch protocols from origins - Allows administrators to specify a list of protocols that can launch an external app from the listed origins without prompting the user.
- Enable command-line flag security warnings - Allows administrators to display or hide security warnings, which appear when potentially dangerous command-line flags try to launch the Enterprise Browser.
- Manage default cookies setting - Allows administrators to manage cookies for a website.
- Manage default pop-ups setting - Allows administrators to manage pop-ups from a website.
- Extension install sources - Allows administrators to specify valid sources for users to install extensions, apps, and themes.
- Disable lookalike warning pages - Allows administrators to specify the preferred domains where lookalike warning pages don't display when the user visits pages on that domain.
- Enable payment method query - Allows administrators to enable websites to check whether the users have saved payment methods.
- Manage saving browser history - Allows administrators to manage the saving of Enterprise browser history.

- Manage search suggestion - Allows administrators to enable or disable search suggestions in the Enterprise browser's address bar.
- Enable export bookmark - Allows administrators to enable an option to export the bookmarks in the Enterprise Browser.
- Force ephemeral profiles - Allows administrators to clear or persist user profile data when users close the Enterprise Browser.

For more information, see the Manage Citrix Enterprise Browser through Global App Configuration service page in the Citrix Enterprise Browser documentation.

For more information on example JSON data, see Example JSON data.

Citrix Endpoint Analysis

With this release, the EPA Client is bundled with the Citrix Workspace app installer. To install the client, Citrix Workspace app must be installed with the command line option `InstallEPAClient`.

Example: `./CitrixworkspaceApp.exe InstallEPAClient`

> **Note:**
>
> EPA isn't installed by default.
>
> In this release, the EPA version packaged is 23.11.1.20.

Deprecation of Citrix Workspace app support

Starting from the 2403 release, support for XenApp Services URLs (also known as PNAgent) for connecting to stores is deprecated. Use Citrix Workspace app to connect to stores using the store URL. For reference, see:

- Deprecation page in the Citrix Workspace app for Windows documentation.
- Deprecation notices page in StoreFront documentation.

Technical Previews in 2403

- Share system audio

For the complete list of Technical Preview features, see the Features in Technical Preview page.

Legacy documentation

For product releases that have reached End of Life (EOL), see Legacy documentation.

Third-party notices

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

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

Fixed issues

Fixed issues in 2507.1

- When using Citrix Workspace app version 2507, administrators might not be able to import Citrix Workspace app template files into Intune.
- Session disappears approximately one minute after launch in CWA 2507
- Session disconnects when using browser settings in Chrome or Edge

Fixed issues in 2507 LTSR

- Some endpoint metrics (such as location, network signal strength etc) might be missing in Director. This issue prevents customer admins from viewing endpoint metrics for users running CWA 2503.10.
- When only a Citrix Enterprise Browser™ update is available, selecting **Close and update** in the auto-update popup might not close or disconnect the ICA session. However, the update continues in the background.
- If GACS settings were configured on the gateway URL, the settings were retrieved only when adding the account for the first time.
- HDX™ sessions might freeze intermittently after a few minutes when the client machine has non-existent or non-responsive printers.
- Browser Content Redirection (BCR) content might display a "Redirecting... You're being redirected to the page" message after expanding the Citrix session to full-screen on 2K and 4K monitors.
- When the DPI of the primary monitor differs from the secondary monitor, the "Custom layout" window might appear misaligned or partially hidden. Clicking the "Custom Layout" window restores it to its normal state.

- When a Local App Access (LAA) session disconnects, you might not receive the "Disconnect Desktop Window" notification.
- When Citrix Workspace™ app is installed as a non-admin user and Local App Access (LAA) is enabled, the toolbar might intermittently disappear in Windowed mode. In Fullscreen mode, the fly-out options of the toolbar might vanish quickly.
- When a Browser Content Redirection (BCR) window gets overlapped by a non-BCR browser window, the BCR window might fail to come to the foreground.
- Client Selective Trust settings might not function properly for desktop launches through webhelper.
- On a client PC with USB device redirection enabled, connecting a composite USB device configured for split interfaces might initially display only the parent device, with child devices appearing in a subsequent notification. As a workaround, wait for the subsequent notification and select the child device for redirection.
- When a USB device is connected to a client PC with USB device redirection enabled and a session is launched, the notification indicating the device can be redirected might remain visible after the session disconnects. Although users can interact with the notification, no action is performed as the session is already closed. The notification automatically times out and disappears after a short duration.
- You might experience difficulty moving the Desktop Viewer toolbar smoothly on touch screen clients when using fingers or a stylus. Additionally, the Desktop Viewer toolbar might disappear when moved with a stylus.
- You might notice visual artifacts when transitioning the DesktopViewer toolbar between vertical and horizontal edges during a VDA session.
- The **Start** button in the **Shortcuts** dropdown menu of the DesktopViewer Toolbar might not function as expected. This issue occurs only when you are using Citrix Workspace app session in windowed mode.
- When using the multiple Virtual Desktops feature in Windows and opening an ICA® session on one desktop, the new DesktopViewer toolbar might appear in preview for all virtual desktops.
- Files might be downloaded from redirected sites to the endpoint when using Browser Content Redirection. This issue occurs from Citrix Workspace app 2402 CU1 hotfix 3.
- Single sign-on to published desktops might fail to launch the Virtual Delivery Agent (VDA) session when the endpoint is registered with Azure Active Directory, the VDA is in hybrid mode (Azure Active Directory and on-premises Active Directory), and the username is passed in AzureAD/usernameInUPN format during launch.

- When switching between "PC Screen Only" and "Extended" mode in a multi-monitor scenario with High DPI set to Yes on the client DPI settings, seamless applications might not render correctly and users might see partial or full black patches on the application.
- When switching to seamless mode with published applications, the endpoint taskbar might become unresponsive.
- Minimizing and maximizing a window on Windows 11 might cause unexpected visual artifacts, such as black areas appearing on the top and left borders of the application.
- Certain HTTPS URLs might not be redirected to the client when using the Host to client redirection feature.
- Creating new non-seamless windows might stop when the number of non-seamless session windows exceeds certain number of windows.
- On endpoints where VBScript is disabled or failed, Citrix Workspace app for Windows installation might fail. This fix removes the VBScript dependency in the installer, ensuring successful installation regardless of VBScript availability.
- You might experience long delays when connecting to the store URL due to shortcut enumeration.
- Legacy email discovery might fail with a certificate not trusted error when the email domain and gateway URL domain do not match.
- The BCR page might flicker when you click outside the browser window (such as on the taskbar or Start menu) and then click back into it.
- When Persistent ICA is enabled, Citrix Workspace app might launch multiple instances of the same application simultaneously.
- When you share a non-standard app like BS Player in Microsoft Teams app sharing, the audience might see a static frame of the previously shared window.
- Web based session launches might fail with the following pop-up error: "Could not load error message".
- When you use host-to-client redirection, you can ignore CRL ping errors on the client by setting the following registry key on the VDA:
  - Path: `HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Citrix\Policies`
  - Type: `REG_DWORD`
  - Name: SFTA
  - Value: 2

Known issues

Known issues in 2507.1

There are no known issues in 2507.1.

Known issues in 2507 LTSR

- If desktop lock feature is enabled in version 2503.2 through command line, desktop lock might not work for standard users after upgrade. This issue doesn't occur when desktop lock is enabled using GPO. As a workaround, during upgrade, enter the "AllowDesktopLockOnMachine EnableDesktopLockForAllStandardUsers" in the command line to re-enable desktop lock. For more information, see Enable Desktop Lock feature using command line parameters.
- Copying and pasting .zip files and directories from the client to the VDA might fail. This issue occurs only when the DDC policy for **Restrict Session Clipboard Write** is active and the **Session Clipboard Write-allowed formats** policy contains *CF_FILE*. As a workaround, do one of the following:
  - Add CF_HDROP format to the Session Clipboard Write-allowed formats policy. Or,
  - Enable the Drag and Drop policy so users can drag and drop files from the client to the VDA instead of copying and pasting.
- When using JAWS 2022 accessibility tool, the Desktop Viewer Toolbar and Disconnect Dialog might have compatibility issues, and the accessibility tool might be unable to read the names of controls as you navigate the UI. As a workaround, you can use the Windows Narrator or JAWS 2025. ,

Features in Technical Preview

Features in Technical Preview are available to use in non-production or limited production environments, and to give customers an opportunity to share feedback. Citrix® does not accept support cases for features in technical preview but welcomes feedback for improving them. Citrix might act on feedback based on its severity, criticality, and importance.

List of features in Technical Preview

The following table lists the features in the technical preview. To provide feedback for any of these features, fill out the respective forms.

TITLE	AVAILABLE FROM VERSION	FEEDBACK FORM (CLICK THE ICON)
Hybrid launch support using GACS for cloud stores	2503	
Browser Profile Sharing	2503	
Enable noise suppression	2503	
Screen recording for specific applications	2409	
Browser Content Redirection and Microsoft Teams Optimization support for ARM64-based devices	2405	
Quick Launch of Disconnected Desktops	2209	
Local App Protection	2210	

Hybrid launch support using GACS for cloud stores

|**Technical Preview from 2503 release** |Feedback form

Starting with version 2503, Citrix Workspace app for Windows supports Global App Configuration Service (GACS) in Hybrid mode for Cloud stores, using the Citrix Workspace launcher. This allows administrators to configure GACS settings through stores added using the browser, streamlining the management of client experiences. This feature is disabled by default for cloud store users. To enable the feature, contact Citrix using the Google form. For more information, see GACS supports hybrid launch.

Browser Profile Sharing

|**Technical Preview from 2503 release** |Feedback form

Browser Content Redirection (BCR) now offers a streamlined user experience with the new **Profile Sharing** feature, enabling VDA-side authentication and cookie sharing. This enhancement eliminates repeated Single Sign-On (SSO) logins, boosting productivity by maintaining authentication and cookie persistence across BCR sessions, even after the BCR window is closed.

This seamless experience further enhances security by ensuring authentication originates from the VDA, not the client.

The **Browser Profile Sharing** feature is supported with **Google authentication** and **Okta**.

Example

- **Previous experience**:

  Previously, opening an authenticated page within BCR required users to re-enter their credentials each time, breaking SSO persistence. SSO was only maintained while the BCR window remained open. Closing and reopening the window forced users to repeat the login process.

- **New experience**:

  With Profile Sharing, users are no longer prompted for credentials. SSO is seamlessly preserved from the VDA browser, providing an improved and uninterrupted experience.

> **Note:**
>
> The feature is not limited to specific providers. Hence, it can be used with other providers as well (for example, Microsoft authentication, PingID). However, current validation is done for the providers specified in the preceding sentence.

Requirements for Technical Preview

- **Citrix Virtual Apps and Desktops™ 2503**
- **Citrix Workspace™ App 2503**
- **Browser Redirection Extension 7.0**

The extension is published in Beta:

Browser Redirection Extension

For more information, see the Citrix Virtual Apps and Desktops documentation.

Enable noise suppression

|**Technical Preview from 2503 release** |Feedback form

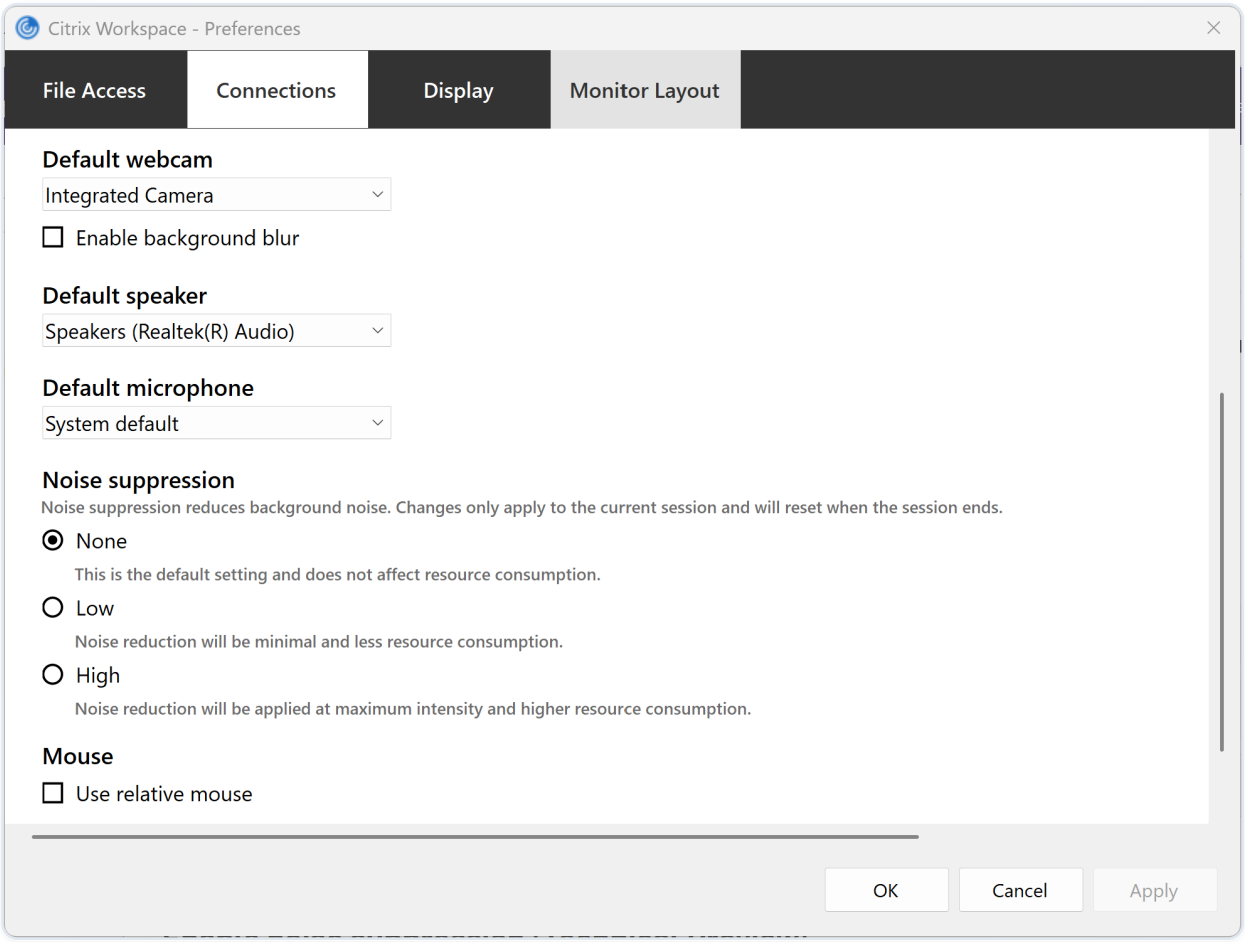
Starting with the 2503 version, Citrix Workspace app now offers improved audio redirection with enhanced noise suppression. This feature reduces background noise, ensuring clearer and more accurate speech, improving the overall communication experience.

Note:

This feature is disabled by default.

To enable this feature, do the following:

1. Navigate to the **Preferences > Connections** section. The **Noise Suppression** screen appears.



2. Select one of the following levels:

   - **None**: This level is the default setting and doesn't use or affect resource consumption.
   - **Low**: Noise reduction is minimal and uses the least resource consumption.
   - **High**: Noise reduction is applied at maximum intensity with the best performance and uses higher resource consumption than the **Low** setting.

3. Click **OK**. The selected configuration is applied.

> **Note:**
>
> Changes apply only to the current session and reset once the session ends.

Screen recording for specific applications

|**Technical Preview from 2503 release** |Feedback form

Citrix Workspace app supports session recording for Secure Private Access scenarios, including Web and SaaS applications accessed through Citrix Enterprise Browser.

You can configure recording policies for Citrix Enterprise Browser. These policies can target specific applications, users, or groups.

When an end user launches an application through Citrix Enterprise Browser, and a matching recording policy applies, the user activities are recorded as a video stream. The video stream is then transferred to the Session Recording server for persistent storage. You can provide and manage the storage locations.

For more information, see Session Recording documentation.

Browser Content Redirection and Microsoft Teams Optimization support for ARM64-based devices

|**Technical Preview from 2405 release** |Feedback form

From the 2405 release, Citrix Workspace app for Windows supports the following features on the ARM64 based devices.

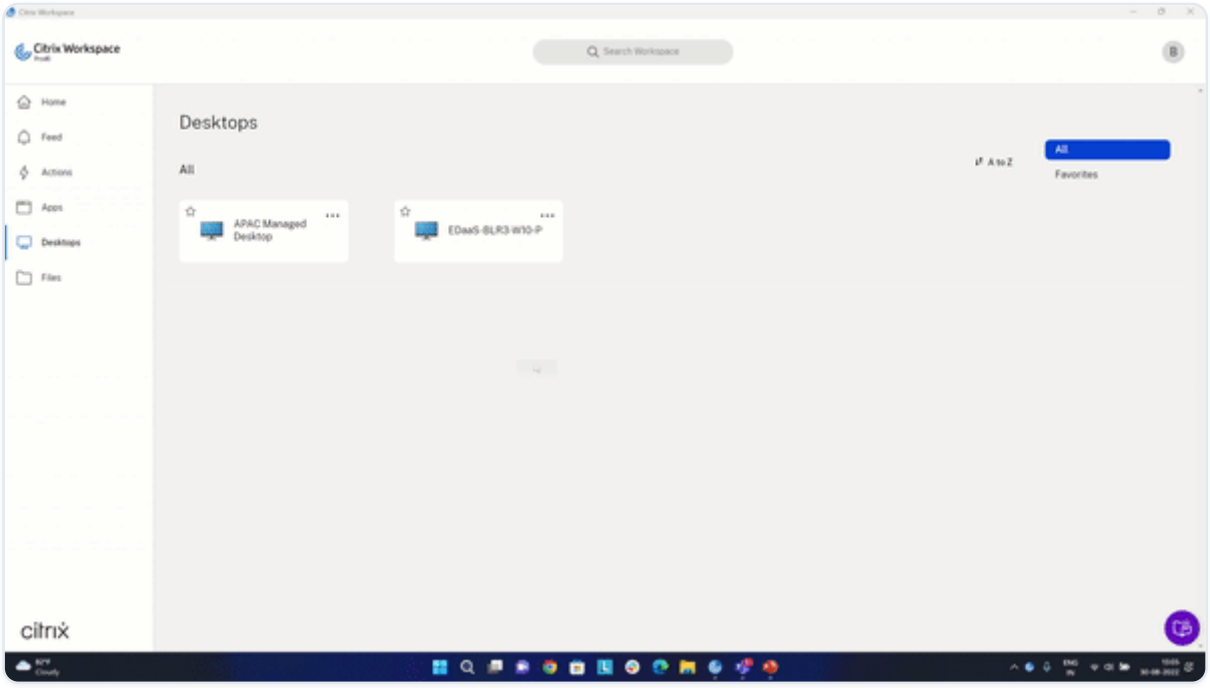
- Browser Content Redirection
- Optimized Microsoft Teams

The prerequisites and system requirements remain the same as installing the app on other architectures. As part of the Citrix Workspace app for Windows installation, the Browser Content Redirection and Microsoft Teams Optimization also get installed.

Quick Launch of Disconnected Desktops

|**Technical Preview from 2209 release** |Feedback form

By enabling this feature, you can open your previously disconnected desktops instantly. Once this feature is enabled, Citrix Workspace app launches the disconnected sessions in hidden mode. The session is instantly presented when you launch the desktop.



Local App Protection

|**Technical Preview from 2210 release** |Feedback form

App Protection offers enhanced security to defend our customers against Keyloggers, accidental and malicious screen capture at endpoints. Currently, App Protection capabilities are only offered for Workspace resources. With Local App Protection, App Protection capabilities are extended to local apps on endpoints. Starting with Citrix Workspace app 2210 for Windows, App Protection can be applied to local apps on Windows devices.

Technical Preview to General Availability (GA)

SERVICE OR FEATURE	GENERAL AVAILABILITY VERSION
Audio Quality Enhancer to improve audio performance	2503.10
Support for TLS protocol version 1.3	2409
Share system audio	2405

SERVICE OR FEATURE	GENERAL AVAILABILITY VERSION
Enhanced domain pass-through for single sign-on	2403
Introducing new installer for Citrix Workspace app	2311.1
Loss tolerant mode for audio	2311.1
Support for an enhanced single sign-on (SSO) experience for web and SaaS apps	2311.1
Improved virtual apps and desktops launch experience	2309
Sustainability initiative from Citrix Workspace app	2309
Plugins management for WebEx plug-in	2305

System requirements and compatibility

Requirements

Hardware requirements

- Minimum 2 GB RAM.
- The following table provides details on the required disk space to install the Citrix Workspace app.

INSTALLATION TYPE	REQUIRED DISK SPACE
Fresh installation	1 GB
Upgrade	1 GB

Note:

- The installer does the check on the disk space only after extracting the installation package.
- When the system is low on disk space during a silent installation, the dialog doesn't appear but the error message is recorded in the following path:
- For 64-bit: `C:\Program Files (x86)\Citrix\Logs\CTXWorkspaceInstallLogs-*`
- For 32-bit: `C:\Program Files\Citrix\Logs\CTXWorkspaceInstallLogs-*`

Software requirements

- Microsoft Edge WebView2 Runtime version 131 or later
- .NET Framework 4.8 and .NET Desktop Runtime 8.0.16 or later (through 8.x). Starting with 2507.1 LTSR CU3, .NET Desktop Runtime 10.0.9 or later
- Microsoft Visual C++ Redistributable 14.51.36231.0 or later

Note:

To handle any security patches from Microsoft or other third party dependent components (for example, .NET Core, .NET Framework, VC redistributable, Edge webview), you can use one of the following methods:

- Enable Windows auto update on client machines
- IT admins to manage patch deployment through tools like SCCM

Microsoft Edge WebView2 requirements

- Citrix Workspace app is packaged with the Evergreen Bootstrapper version of Microsoft Edge WebView2 Runtime.
- Citrix Workspace app installer can install Microsoft Edge WebView2 Runtime during the Citrix Workspace app installation. However, for this installation, you must be connected to the internet. Alternatively, you can install the offline Microsoft Edge WebView2 Runtime Evergreen Standalone Installer package based on the Windows OS platform before installing Citrix Workspace app.
- The device must have access to the following URLs:
  - `https://*.dl.delivery.mp.microsoft.com` to download Microsoft Edge WebView2 Runtime during the Citrix Workspace app installation. For more information, see Allow list for Microsoft Edge endpoints.
  - `https://msedge.api.cdp.microsoft.com` to check for Microsoft Edge WebView2 Runtime update
  - Internet connection

Note:

When you try to install or upgrade Citrix Workspace app with non-administrator privileges and Microsoft Edge WebView2 Runtime isn't present, the installation stops with the following message:

'You must be logged on as an administrator to install the following prerequisite packages:

Edge Webview 2 Runtime'

.NET requirements

Prerequisites

- .NET Framework 4.8 and the x86 version of .NET Desktop Runtime are required for Citrix Workspace app 2409 or later. For releases up to 2507.1 LTSR CU2, use 8.0.16 or later through 8.x. Starting with 2507.1 LTSR CU3, use 10.0.9 or later. You must install the x86 version even on x64 systems.
- In installing .NET as part of Citrix Workspace app installation, ensure internet connection.
- Administrator privileges

Note:

The installation fails when you try to install or upgrade Citrix Workspace app without administrator privileges and the required prerequisites are not present on the system.

Installation methods

.NET VERSION	HOW TO DEPLOY IT?
Citrix Workspace app 1904 or later requires .NET Framework 4.8. Along with .NET Framework 4.8, Citrix Workspace app 2409 or later requires the x86 version of .NET Desktop Runtime for both x86 and x64 systems: 8.0.16 or later (through 8.x) up to 2507.1 LTSR CU2, and 10.0.9 or later starting with 2507.1 LTSR CU3.	Method 1: Citrix Workspace app installs .NET Framework 4.8 and .NET Desktop Runtime during app installation. This is an online installation and requires internet connectivity. The device must have access to the downloadplugins.citrix.com domain URL. For releases up to 2507.1 LTSR CU2, use .NET Desktop Runtime 8.0.16 or later (through 8.x). Starting with 2507.1 LTSR CU3, use .NET Desktop Runtime 10.0.9 or later.
	Method 2: For Devices that don't have internet connectivity, admins have an option to download an offline installer for Citrix Workspace app available at the Downloads page. Also, the administrator can install this

.NET VERSION	HOW TO DEPLOY IT?
	requirement using a deployment method, for example, SCCM.
	Method 3: Admins can install .NET Framework 4.8 and .NET Desktop Runtime 10.0.9 and .NET Desktop Runtime 8.0.16 from the Microsoft site separately before installing Citrix Workspace app. It is recommended to download the latest version of .NET Desktop Runtime.
	Note: Perform a Microsoft update for Windows to ensure the .NET version is updated to the latest version. Citrix Workspace app for Windows supports the latest .NET version.

Compatibility with the higher versions of .NET

Citrix Workspace app for Windows version 2405 or later is compatible with the higher versions of .NET that are supported on your system. To ensure this compatibility, Citrix Workspace app follows these installation rules:

- If .NET isn't installed, or if the installed version is lower than the required baseline, Citrix Workspace app installs the required .NET Desktop Runtime during installation.
- If you install any supported higher version of .NET, Citrix Workspace app is compatible with the highest available .NET version (up to 8.x).

Microsoft Visual C++ Redistributable requirements

Citrix Workspace app requires the latest version of Microsoft Visual C++ Redistributable. The minimum version required for Citrix Workspace app for Windows 2508 or later is 14.51.36231.0 or later.

> **Note:**

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

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

> **Note:**

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

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

Connectivity requirements

Feature flag management

Feature flags are used to enable or disable features dynamically. If an issue occurs with Citrix Workspace app in production, the affected feature can be disabled dynamically, even after the feature is shipped.

No configurations are needed to enable traffic for feature management, except when a firewall or proxy is blocking outbound traffic. In such cases, you need to enable traffic using specific URLs or IP addresses, depending on your policy requirements.

Enable traffic for feature flag management

From Citrix Workspace app version 2409 onwards:

To ensure optimal functionality and access to preview features, you need to enable traffic to the URL `features.netscalergateway.net`.

> **Note:**

> Adding the preceding URL to the allow list is essential for optimal use of Citrix feature flags and is supported starting with version 2409 of the Citrix Workspace app for Windows.

Ports

For information on the required ports, see Common Citrix Communication Ports.

Compatibility matrix

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

Note:

- The Citrix Gateway End-Point Analysis Plug-in (EPA) is supported on Citrix Workspace. On the native Citrix Workspace app, it's supported only when using nFactor authentication. For more information, see Configure pre-auth and post-auth EPA scan as a factor in nFactor authentication in the Citrix ADC documentation.
- Citrix Workspace app installation on Windows is supported only when the customers have mainstream or extended support from Microsoft.
- Citrix Workspace app for Windows is supported only in emulator mode on the Windows ARM64 operating system.
- Once a Windows 10 version reaches End of Service that version is no longer serviced or supported by the Microsoft. Citrix supports running its software only on an operating system that its manufacturer supports. For information about Windows 10 End of Service, see Microsoft's Windows Lifecycle Fact Sheet.

Citrix Workspace app for Windows is compatible with the following Windows Operating Systems:

OPERATING SYSTEM
Windows 11 IoT Enterprise LTSC 2024
Windows 11
Windows 10 Enterprise (32-bit and 64-bit Editions). For more information about compatible Windows 10 versions, see Windows 10 Compatibility with Citrix Workspace app for Windows.

OPERATING SYSTEM
Windows 10 Enterprise LTSC 2021
Windows 10 (Home edition*, Pro)
Windows Server 2022
Windows Server 2019
Windows Server 2025

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

Windows 10 or 11 Compatibility with Citrix Workspace app for Windows

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

WINDOWS 11 VERSION NUMBER	BUILD NUMBER	CITRIX WORKSPACE APP VERSION
25H2	26200	2507.1 CU1 and later
24H2	26100	2409 and later
23H2	22631	2311 and later
22H2	22621	2209 and later
21H2	22000	2109.1 and later

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

WINDOWS 10 VERSION NUMBER	BUILD NUMBER	CITRIX WORKSPACE APP VERSION
22H2	19045	2206 and later
21H2	19044	2112.1 and later

CITRIX WORKSPACE™ APP FOR WINDOWS

WINDOWS 10 VERSION NUMBER	BUILD NUMBER	CITRIX WORKSPACE APP VERSION
21H1	19043.928	2106 and later
20H2	19042.508	2012 and later
2004	19041.113	2006.1 and later
1909	18363.418	1911 and later
1903	18362.116	1909 and later
1809	17763.107	1812 and later
1803	17134.376	1808 and later

Note:

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

Install and uninstall

You can download Citrix Workspace app from the Download page of Citrix or from your company's download page (if available).

You can install the package by:

- Running an interactive Windows-based installation wizard.

  Or

- Typing the installer file name, installation commands, and installation properties using the command-line interface. For information about installing Citrix Workspace app using a command-line interface, see Using command-line parameters.

Note:

- Verify that you have installed all the required system requirements, as mentioned at System requirements section.
- Use the `CitrixWorkspaceApp.exe /CleanInstall` command when upgrading to a newer version of Citrix Workspace app. For downgrades, it is recommended to uninstall Citrix Workspace app first.

Installation with administrator and non-administrator privileges:

Both users and administrators can install Citrix Workspace app. Administrator privileges are required only when using pass-through authentication, single sign-on, App Protection, and Microsoft Teams VDI plug-in with Citrix Workspace app for Windows.

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

	INSTALLATION FOLDER	INSTALLATION TYPE
Administrator	For 64-bit: C:\Program Files (x86)\Citrix\ICA Client and for 32-bit: C:\Program Files\Citrix\ICA Client	Per-system installation
User	%USERPROFILE% \AppData\Local\Citrix\ICA Client	Per-user installation

Note:

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

Command to cleanup and install Citrix Workspace app

Use the `/CleanInstall` command to cleanup any leftover traces such as files and registry values from a previous uninstall and then freshly install the new version of the Citrix Workspace app.

For example:

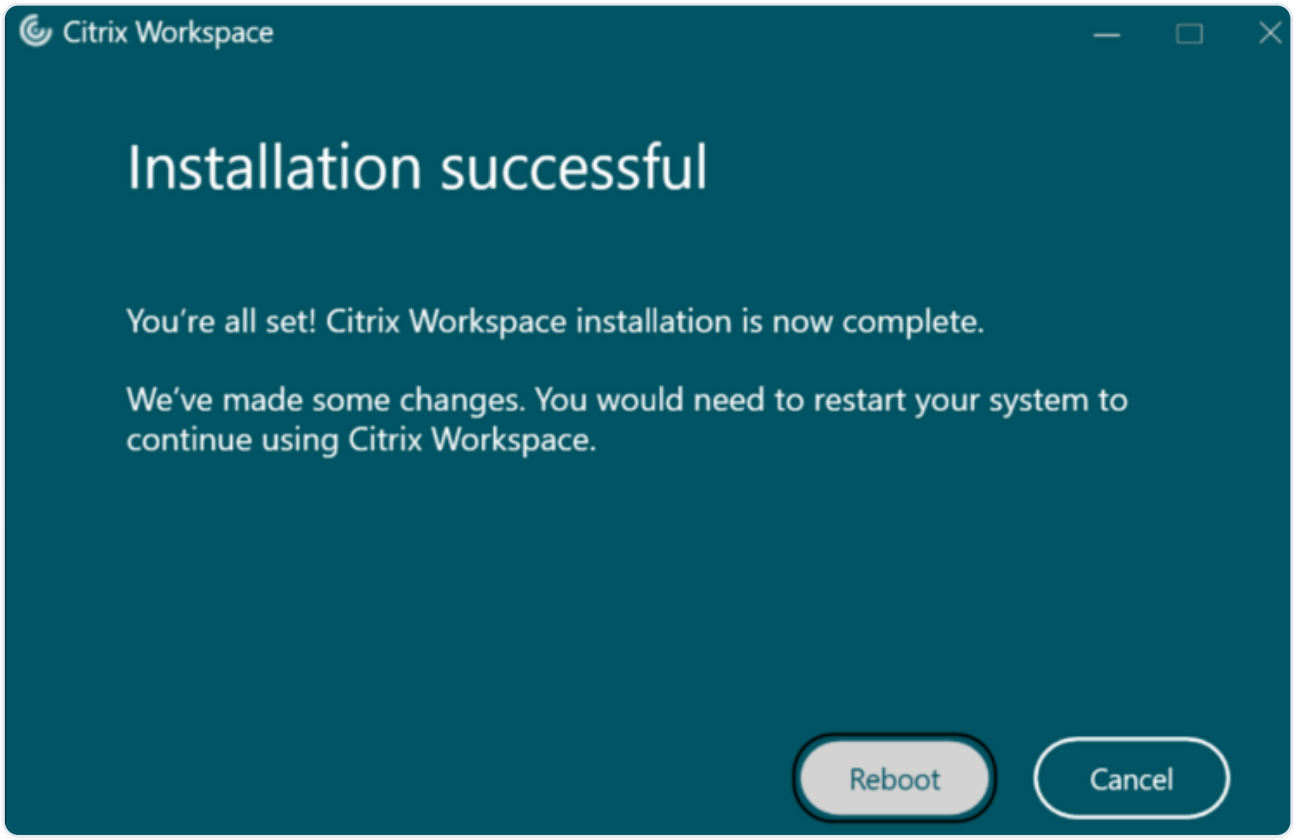
```
CitrixWorkspaceApp.exe /CleanInstall
```

Note:

The difference between the `forceinstall` and `cleaninstall` commands is that `forceinstall` runs in case of an unsupported version upgrade or any failure, whereas `cleaninstall` always cleans up before performing the required action, whether it is an install or an upgrade.

Enhanced installation process for Citrix Workspace™ app with App Protection

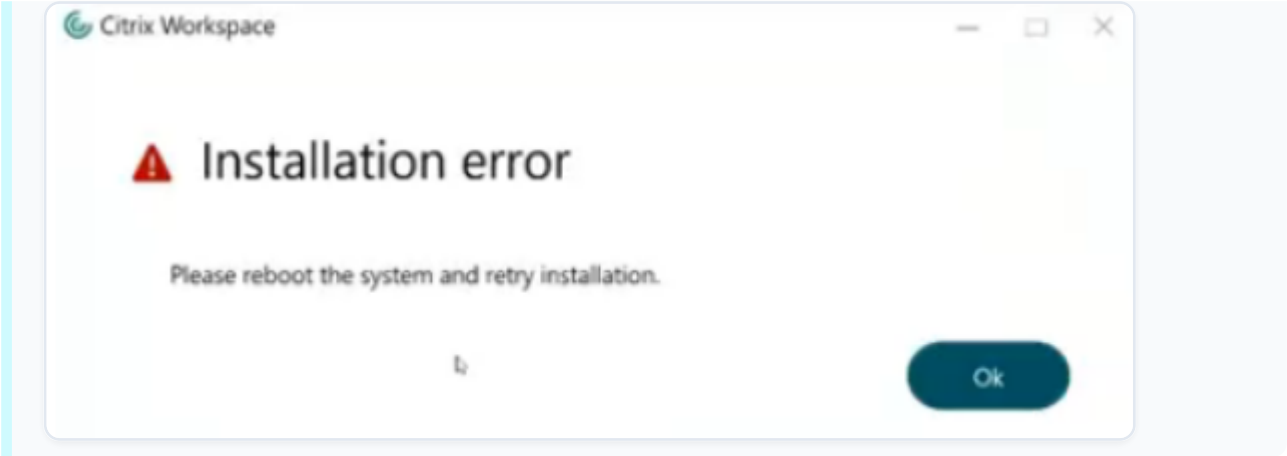
Previously, when App Protection was enabled, the `/cleanInstall` switch was not supported, and the user had to manually uninstall and reboot the machine before retrying installation. Starting with the 2503 version, when App Protection is enabled and the `/CleanInstall` command is run, Citrix Workspace app automatically uninstalls, reboots the machine based on user selection, and reinstalls the app during the reboot. The following message appears during the process:



- If the user clicks **Reboot**, Citrix Workspace app reinstalls during the reboot.
- If the user clicks **Cancel**, Citrix Workspace app will be installed upon the next reboot. As a result, Citrix Workspace app is not available when searching for the app in the system.

Note:

- For silent installations, Citrix Workspace app is available only after the next user-initiated reboot.
- If the user retries the installation before reboot, the following prompt appears to reboot the system:

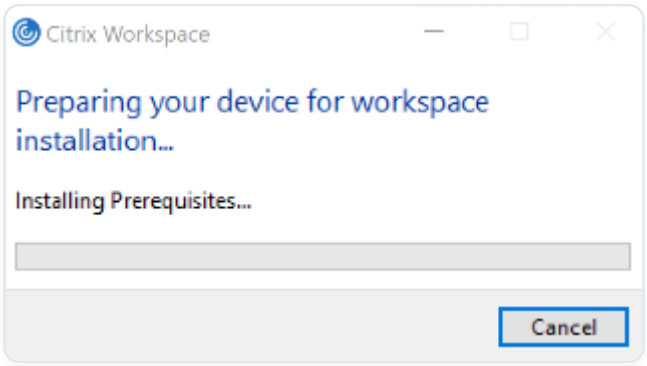


User interface based installation

You can install Citrix Workspace app for Windows by manually running the **CitrixWorkspaceApp.exe** installer package.

1. Launch the `CitrixWorkspaceApp.exe` file.

   The system verifies the prerequisites required for Citrix Workspace app and if requires, installs it automatically.

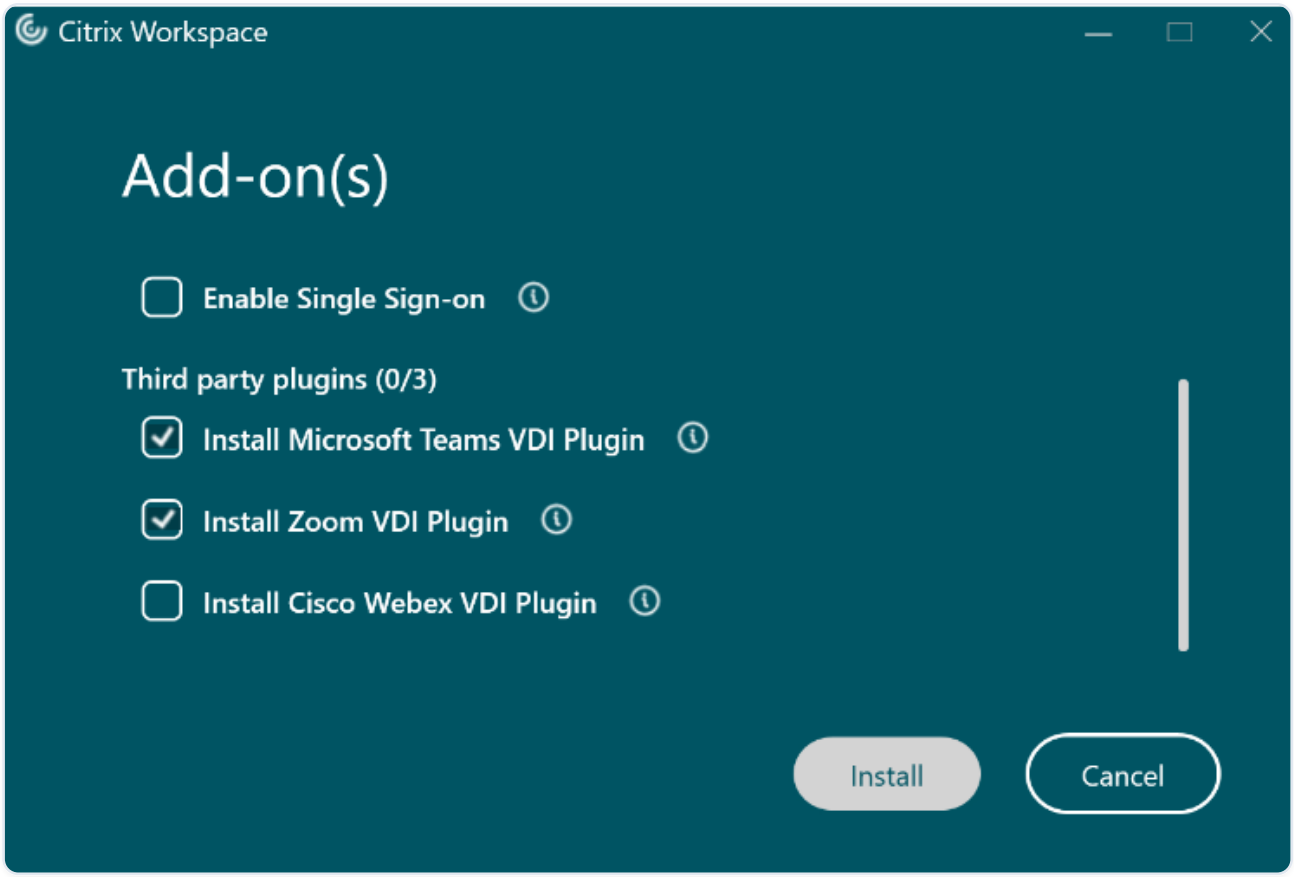
   

   After installing the prerequisites, the **Welcome to Citrix Workspace Installer** screen appears.

2. Click **Continue**. The **Citrix License Agreement** page appears.
3. Read and accept the Citrix License Agreement and continue with the installation. Citrix Workspace app installation continues and successfully completes.
4. When installing with administrator privileges, you can choose the following from the **Add-on(s)** page:

   - Start App Protection after installation
   - Enable single sign-on
   - Install Microsoft Teams VDI Plugin

- Install Zoom VDI Plugin
- Install Cisco WebEx VDI plugin



Citrix Workspace app installation continues and successfully completes.

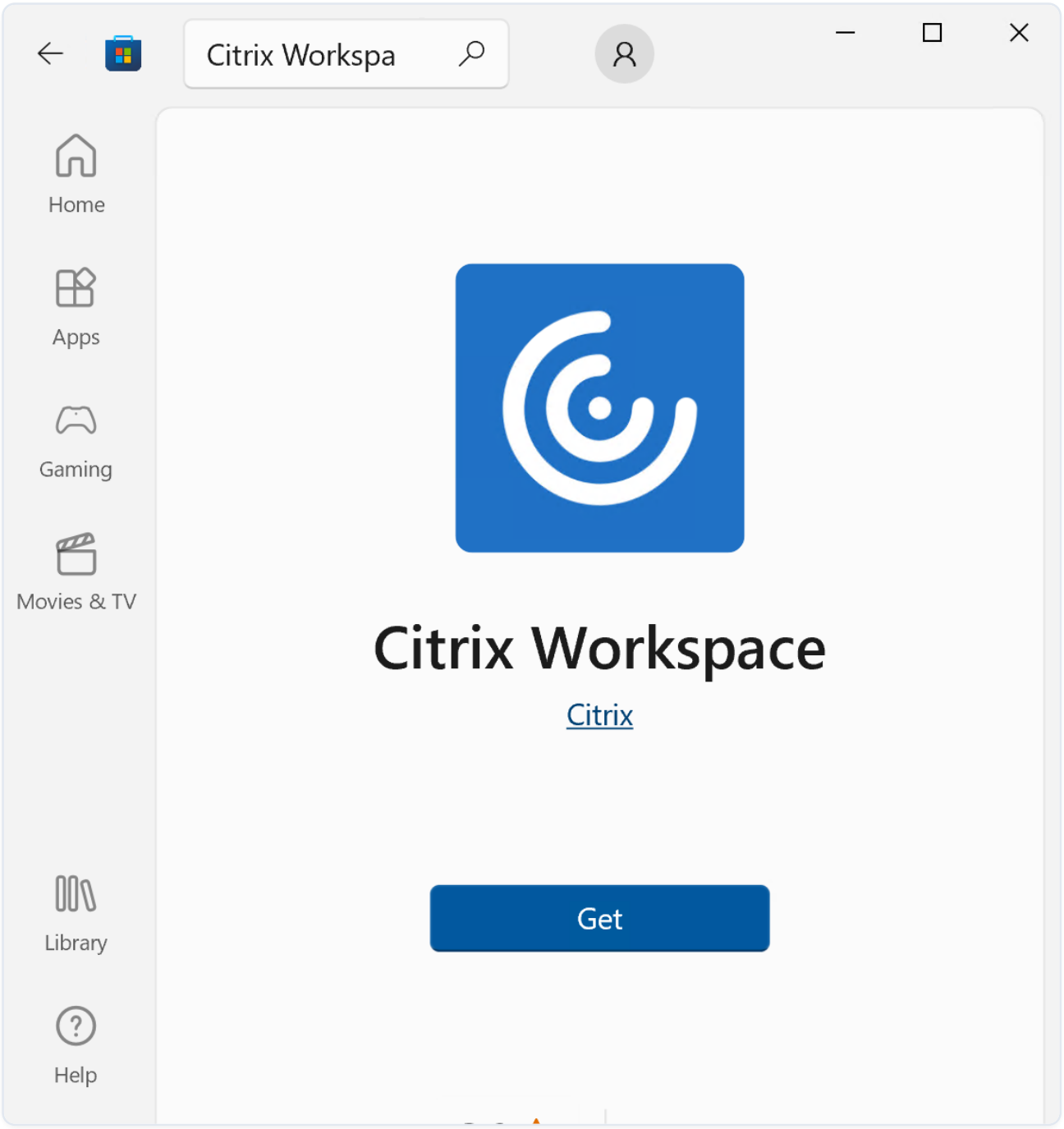


Important:

Starting with Citrix Workspace app for Windows 2311.1 version, the `TrolleyExpress` is replaced with `CWAInstaller-<date and timestamp>`. For example, the log is recorded at `C:\Program Files (x86)\Citrix\Logs\CTXWorkspaceInstallLogs-20231225-093441`.

Using Windows Store

1. Navigate to Microsoft Store.
2. Search for Citrix Workspace.



1. Click **Get**. Citrix Workspace app is installed.

Command-line based installation

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

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

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

The available installation commands and properties are as follows:

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

List of command-line parameters

The parameters are broadly classified as follows:

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

Common parameters

COMMAND	DESCRIPTION
`?` Or `help`	Lists all the installation commands and properties.
`/silent`	Disables installation dialogs and prompts during installation.
`/forceinstall`	This switch is effective when cleaning up any existing configuration or entries of Citrix Workspace app in the system. Use this switch when upgrading from an unsupported version of Citrix Workspace app version and when the installation or upgrade is unsuccessful.

Note:

The `forceinstall` switch is the replacement for the `rcu` switch. The `rcu` switch is deprecated as of Version 1909. For more information, see Deprecation.

The difference between the `forceinstall` and `cleaninstall` commands is that `forceinstall` runs in case of an unsupported version upgrade or any failure, whereas `cleaninstall` always cleans up before performing the required action, whether it is an install or an upgrade.

Auto-update parameters

Detect available update

- Command: `AutoUpdateCheck`
- Description: This command indicates that Citrix Workspace app detects when an update is available.

The possible values are the following:

AUTOUPDATECHECK COMMAND VALUES	DESCRIPTION	EXAMPLE
Auto (default)	You're notified when an update is available.	`CitrixWorkspaceApp.exe AutoUpdateCheck=auto`.
Manual	You aren't notified when an update is available. Check for updates manually.	`CitrixWorkspaceApp.exe AutoUpdateCheck=manual`
Disabled	Disables auto-updates.	`CitrixWorkspaceApp.exe AutoUpdateCheck=disabled` .

Note:

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

Select the version for update

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

The possible values are the following:

AUTOUPDATESTREAM COMMAND VALUE	DESCRIPTION	EXAMPLE
LTSR	Auto-updates to Long Term Service Release cumulative updates only.	`CitrixWorkspaceApp.exe AutoUpdateStream=LTSR`.
Current	Auto-updates to the latest version of Citrix Workspace app.	`CitrixWorkspaceApp.exe AutoUpdateStream=Current`

Defer notifications for update

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

The possible values are the following:

DEFERUPDATECOUNT COMMAND VALUE	DESCRIPTION	EXAMPLE
-1(default)	Allows deferring notifications any number of times	`CitrixWorkspaceApp.exe DeferUpdateCount=-1`
0	Indicates that you receive one notification (only) for every available update. Doesn't remind you again about the update.	`CitrixWorkspaceApp.exe DeferUpdateCount=0`
Any other number 'n'	• Allows deferring notification 'n' number of times. The **Remind me**	`CitrixWorkspaceApp.exe DeferUpdateCount=<n>`

DEFERUPDATECOUNT COMMAND VALUE	DESCRIPTION	EXAMPLE
	later option is displayed in the 'n' count.	

Note:

Starting with Citrix Workspace app for Windows version 2207, the auto-update feature is improved and the `DeferUpdatCount` parameter in not applicable.

Set rollout priority

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

The possible values are the following:

AUROLLOUTPRIORITY COMMAND VALUE	DESCRIPTION	EXAMPLE
Auto (default)	You receive the updates during the delivery period as configured by Citrix.	`CitrixWorkspaceApp.exe AURolloutPriority=Auto`
Fast	You receive the updates at the beginning of the delivery period.	`CitrixWorkspaceApp.exe AURolloutPriority=Fast`
Medium	You receive the updates at the mid-delivery period.	`CitrixWorkspaceApp.exe AURolloutPriority=Medium`
Slow	You receive the updates at the end of the delivery period.	`CitrixWorkspaceApp.exe AURolloutPriority=Slow`

Store configuration parameters

Configure store

- Command: `ALLOWADDSTORE`
- Description: Allows you to configure the stores (HTTP or https) based on the specified parameter.

The possible values are the following:

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

Save the store credentials locally

- Command: `ALLOWSAVEPWD`
- Description: Allows you to save the store credentials locally. This parameter applies only to stores using the Citrix Workspace app protocol.

The possible values are the following:

ALLOWSAVEPWD COMMAND VALUE	DESCRIPTION	EXAMPLE
S (default)	Allows saving the password for secure stores only (configured with HTTPS).	`CitrixWorkspaceApp.exe ALLOWSAVEPWD=S`

ALLOWSAVEPWD COMMAND VALUE	DESCRIPTION	EXAMPLE
N	Does not allow saving the password.	`CitrixWorkspaceApp.exe ALLOWSAVEPWD=N`
A	Allows saving the password for both secure stores (HTTPS) and non-secure stores (HTTP).	`CitrixWorkspaceApp.exe ALLOWSAVEPWD=A`

Examples of store configuration using command-line installation

To specify the StoreFront store URL:

```
CitrixWorkspaceApp.exe /silent

STORE0="AppStore;https://testserver.net/Citrix/MyStore/discovery;on;HR App Store"
```

To specify the Citrix Gateway store URL:

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

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

Note:

- The Citrix Gateway store URL configured using this method does not support the PNA Services Sites that are using Citrix Gateway.
- The "Discovery" parameter is not required when specifying a Citrix Gateway store URL.

To configure multiple stores:

```
CitrixWorkspaceApp.exe  STORE0="StoreFront Store;https://testserver.net/
Citrix/MyBackupStore/discovery;on; StoreFrontStore"



STORE1="NetScaler Store;https://ag.mycompany.com#Storename;On;NetScaler
Store"
```

Note:

It's mandatory to include `discovery` in the store URL for successful pass-through authentication.

The following table provides description for the parameters of store URL:

PARAMETER	DESCRIPTION
Store name	The name that the user sees for the store.
Store URL	The URL for the store.
Store enabled state	The state can be on or off.
Store description	The description that the user sees for the store.

Example for StoreFront™:

`SalesStore;https://sales.mycompany.com/Citrix/Store/discovery;On;Store` for Sales staff.

Install parameters

Start App Protection

- Command: `startAppProtection`
- Description: Start App Protection component and provides enhanced security by restricting the ability of clients to be compromised by keylogging and screen-capturing malware.

- Example: `CitrixWorkspaceApp.exe startAppProtection`

For more information, see the App Protection documentation.

> **Note:**
>
> The `startAppProtection` switch is the replacement for the `includeAppProtection` switch. The `includeAppProtection` switch is deprecated as of Version 2212. For more information, see Deprecation.

Exclude Citrix Enterprise Browser binaries

- Command: Run the following command to exclude Citrix Enterprise Browser™

```
CitrixWorkspaceapp.exe
ADDLOCAL=ReceiverInside,ICA_Client,BCR_Client,USB,DesktopViewer,AM,SSON,Se
lfService,WebHelper
```

- Description: Excludes the Citrix Enterprise Browser binaries.

You can exclude the Citrix Enterprise Browser binaries only in the following cases:

- Fresh install
- Upgrade from a version that doesn't include the Citrix Enterprise Browser binaries.

Exclude EPA Client from automatic installation

- Command: `CitrixWorkspaceApp.exe InstallEPAClient=N`
- Description: Stops the automatic installation of the EPA Client.
- For example, using the following command

```
CitrixWorkspaceapp.exe
ADDLOCAL=ReceiverInside,ICA_Client,BCR_Client,USB,DesktopViewer,AM,SSON,Se
lfService,WebHelper InstallEPAClient=N
```

You can exclude the EPA in the following cases:

- Fresh install
- Upgrade from a version that doesn't include the EPA.

Specify custom installation directory

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

> **Note:**
>
> The **Program Files** folder is protected by the operating system. If you want to use a custom folder other than Program Files, ensure that the folder has the right permission and it is protected.

Install one or more of the specific components

- Command: `ADDLOCAL`
- Description: Use the `ADDLOCAL` key to install one or more of the specific components of the Citrix Workspace app. Using this key, if you install any specific components, the Citrix Workspace app installs all the mandatory components by default.

> **Note:**
>
> When upgrading the Citrix Workspace app, the installer does not honor exclusion commands (such as, `BCR_Client`) for components that are already present in the base version. To remove a component during an upgrade process, fully uninstall the existing Citrix Workspace app before installing the new version with the required exclusion parameters.

> We recommended you to use the `ADDLOCAL` key only if you want to install any of the specific components of Citrix Workspace app. By default, if no `ADDLOCAL` parameter is specified, all the supported components are installed while installing the Citrix Workspace app.

> The following table lists the components that the `ADDLOCAL` key supports:

ADDLOCAL KEY	COMPONENT NAME	DESCRIPTION
`ReceiverInside`	Receiver	Provides workspace SDK services to the Self-service plug-in.
`ICA_Client`	HDX™ Engine	This component handles the ICA file or session launch process.
`BCR_Client`	BCR client	Plug-in to handle browser content redirection.
`USB`	USB Client	Plug-in to take care of the USB redirection.
`DesktopViewer`	Desktop Viewer Client	UI framework for virtual desktop.
`AM`	AuthManager	Authentication Manager - Authorizes user to Citrix Workspace app.
`SSON`	SSON	Single sign-on component – Supports single sign-on.
`SELFSERVICE`	Self-service	Plug-in for the Citrix Workspace for native launch.
`WebHelper`	Web Helper	Helper to connect browser with native workspace app.
`CitrixEnterpriseBrowser`	Browser	Native browser that enables users to open web or SaaS apps from Citrix Workspace app in a secure manner.

For example, using the following command, you can install the components mentioned in the command:

```
CitrixWorkspaceapp.exe
ADDLOCAL=ReceiverInside,ICA_Client,BCR_Client,USB,DesktopViewer,AM,SSON,Se
lfService,WebHelper,CitrixEnterpriseBrowser
```

Note:

Starting with version 2212, the App Protection feature is installed by default. As a result, `AppProtection` is no longer a valid option for the `ADDLOCAL` command.

Limitation:

When you install Citrix Workspace app using ADDLOCAL parameters, the **Devices** and **Preferences** window might not respond from the **Connection Center**. This issue occurs only when you install Citrix Workspace app without the `DesktopViewer` parameter. As a workaround, include the `DesktopViewer` parameter as well.

Install plug-ins

- Command: `ADDONS`
- Description: Use the `ADDONS` key to install one or more of the specific plug-ins of the Citrix Workspace app.

The following table lists the components that the `ADDONS` key supports:

ADDONS KEY	COMPONENT NAME	DESCRIPTION
`ZoomVDIPlugin`	Zoom VDI Plug-in	Installs Zoom VDI Plug-in manager as part of the Citrix Workspace app installation
`WebexVDIPlugin`	WebEx VDI Plug-in	Installs WebEx VDI Plug-in manager as part of the Citrix Workspace app installation

For example, using the following command, you can install the plug-ins mentioned in the command:

```
CitrixWorkspaceapp.exe ADDONS=ZoomVDIPlugin,WebexVDIPlugin
```

Install Citrix Casting™

> **Important:**
>
> For Citrix Workspace app LTSR version 2402 and later, Citrix casting cannot be installed even with the `IncludeCitrixCasting` command. To use this feature, you must use an older version of Citrix Workspace app. For more information, see the Deprecation page.

- Command: `IncludeCitrixCasting`
- Description: Installs Citrix Casting during installation.

For more information on Citrix Casting, see Citrix Casting.

UberAgent parameters

- Command: `InstallUberAgent`
- Description: The UberAgent add-on delivers advanced monitoring and diagnostics for Citrix Workspace app, providing detailed insights into user experience and application performance. This integration is available exclusively on managed devices, streamlining deployment and reducing administrative overhead.

Using the following command-line installation:

Use the command `/InstallUberAgent` to install or upgrade the UberAgent plugin. Use the command `/InstallUberAgent /SkipUberAgentUpgrade` to install the plugin without upgrading it if UberAgent is already present. This option is ideal for VDAs or devices where UberAgent deployment is managed separately from Citrix Workspace app.

> **Note:**
>
> This component can be installed through command-line only.

> UberAgent 7.5.1 and higher versions support only x64 (64-bit) platforms. You cannot install or use UberAgent on x86 (32-bit) machines.

HDX features parameters

Set bidirectional content redirection

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

The possible values are the following:

ALLOW_BIDIRCONTENTREDIRECTION COMMAND VALUE	DESCRIPTION	EXAMPLE
0 (default)	Indicates that the bidirectional content redirection is disabled.	`CitrixWorkspaceApp.exe ALLOW_BIDIRCONTENTREDIRECTION=0`
1	Indicates that the bidirectional content redirection is enabled.	`CitrixWorkspaceApp.exe ALLOW_BIDIRCONTENTREDIRECTION=1`

Set local app access

- Command: `FORCE_LAA`
- Description: Indicates that Citrix Workspace app is installed with the client-side Local App Access component. Install the workspace app with administrator privileges for this component to work. For more information, see the Local App Access section in the Citrix Virtual Apps and Desktops documentation.

The possible values are the following:

FORCE_LAA COMMAND VALUE	DESCRIPTION	EXAMPLE
0 (default)	Indicates that the Local App Access component isn't installed.	`CitrixWorkspaceApp.exe FORCE_LAA =0`

FORCE_LAA COMMAND VALUE	DESCRIPTION	EXAMPLE
1	Indicates that the client-end Local App Access component is installed.	`CitrixWorkspaceApp.exe FORCE_LAA =1`

Set URL redirection feature on the user device

- Command: `ALLOW_CLIENTHOSTEDAPPSURL`
- Description: Enables the URL redirection feature on the user device. For more information, see the Local App Access section in the Citrix Virtual Apps and Desktops documentation.

The possible values are the following:

ALLOW_CLIENTHOSTEDAPPSURL COMMAND VALUE	DESCRIPTION	EXAMPLE
0 (default)	Disables the URL redirection feature on the user device.	`CitrixWorkspaceApp.exe ALLOW_CLIENTHOSTEDAPPSURL=0`
1	Enables the URL redirection feature on the user devices.	`CitrixWorkspaceApp.exe ALLOW_CLIENTHOSTEDAPPSURL=1`

Display icons for documents or files

- Command: `LEGACYFTAICONS`
- Description: Specifies if you want to display icons for documents or files that have file type association with subscribed applications.

The possible values are the following:

LEGACYFTAICONS COMMAND VALUE	DESCRIPTION	EXAMPLE
False (default)	Display icons for documents or files that have file type associations with subscribed applications. When set to false, the operation system	`CitrixWorkspaceApp.exe LEGACYFTAICONS=False`

LEGACYFTAICONS COMMAND VALUE	DESCRIPTION	EXAMPLE
	generates an icon for the document that doesn't have a specific icon assigned to it. The icon generated by the operation system is a generic icon overlaid with a smaller version of the application icon.	
True	Doesn't display icons for documents or files that have file type associations with subscribed applications.	`CitrixWorkspaceApp.exe LEGACYFTAICONS=True`

Preference and user interface parameters

Specify the directory for the shortcuts on the Start menu and desktop

COMMAND VALUE	DESCRIPTION	DIRECTORY NAME	EXAMPLE
`CitrixWorkspaceApp.exe STARTMENUDIR`	Specifies the directory for the shortcuts in the Start menu.	By default, applications appear under **Start** > **All Programs**. You can specify the relative path of the shortcuts in the `Programs` folder.	To place shortcuts under **Start** > **All Programs** > **Workspace**, specify `STARTMENUDIR=Workspace`.
`CitrixWorkspaceApp.exe DESKTOPDIR`	Specifies the directory for shortcuts on the Desktop.	You can specify the relative path of the shortcuts.	To place shortcuts under **Start > All Programs > Workspace**, specify `DESKTOPDIR=Workspace`.

Note:

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

Control access to the self-service

- Command: `SELFSERVICEMODE`
- Description: Controls access to the self-service Citrix Workspace app user interface.

The possible values are the following:

SELFSERVICEMODE COMMAND VALUE	DESCRIPTION	EXAMPLE
True	Indicates that the user has access to the self-service user interface.	`CitrixWorkspaceApp.exe SELFSERVICEMODE=True`
False	Indicates that the user does not have access to the self-service user interface.	`CitrixWorkspaceApp.exe SELFSERVICEMODE=False`

Control session pre-launch

- Command: `ENABLEPRELAUNCH`
- Description: Controls session pre-launch. For more information, see Application launch time.

The possible values are the following:

ENABLEPRELAUNCH COMMAND VALUE	DESCRIPTION	EXAMPLE
True	Indicates that session pre-launch is enabled.	`CitrixWorkspaceApp.exe ENABLEPRELAUNCH=True`
False	Indicates that session pre-launch is disabled.	`CitrixWorkspaceApp.exe ENABLEPRELAUNCH=False`

Hide Shortcuts and Reconnect option

- Command: `DisableSetting`

- Description: Hides the **Shortcuts and Reconnect** option from being displayed in the **Advanced Preferences** sheet. For more information, see Hiding specific settings from the Advanced Preferences sheet.

The possible values are the following:

DISABLESETTING COMMAND VALUE	DESCRIPTION	EXAMPLE
0 (default)	Displays both **Shortcuts** and **Reconnect** options in the Advanced Preferences sheet.	`CitrixWorkspaceApp.exe DisableSetting=0`
1	Displays only the **Reconnect** option in the Advanced Preferences sheet.	`CitrixWorkspaceApp.exe DisableSetting=1`
2	Displays only the **Shortcuts** option in the Advanced Preferences sheet.	`CitrixWorkspaceApp.exe DisableSetting=2`
3	Both **Shortcuts** and **Reconnect** options are hidden from the Advanced Preferences sheet.	`CitrixWorkspaceApp.exe DisableSetting=3`

Enable Customer Experience Improvement Program

- Command: `EnableCEIP`
- Description: Indicates your participation in the Customer Experience Improvement Program (CEIP). For more information, see CEIP.

The possible values are the following:

ENABLECEIPCOMMAND VALUE	DESCRIPTION	EXAMPLE
True (default)	Opt in to the Citrix Customer Improvement Program (CEIP)	`CitrixWorkspaceApp.exe EnableCEIP=True`
False	Opt out of the Citrix Customer Improvement Program	`CitrixWorkspaceApp.exe EnableCEIP=False`

Enable always-on tracing

- Command: `EnableTracing`
- Description: Controls the **Always-on tracing** feature.

The possible values are the following:

ENABLETRACING COMMAND VALUE	DESCRIPTION	EXAMPLE
True (default)	Enables the **Always-on tracing** feature.	`CitrixWorkspaceApp.exe EnableTracing=true`
False	Disables the **Always-on tracing** feature.	`CitrixWorkspaceApp.exe EnableTracing=false`

Specify the name to identify the user device

- Command: `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%`.
- Example: `CitrixReceiver.exe CLIENT_NAME=%COMPUTERNAME%`.

Set client name same as the computer name

- Command: `ENABLE_DYNAMIC_CLIENT_NAME`
- Description: Allows the client name to be the same as the computer name. When you change the computer name, the client name changes too.

The possible values are the following:

ENABLE_DYNAMIC_CLIENT_NAME COMMAND VALUE	DESCRIPTION	EXAMPLE
Yes (default)	Allows the client name to be the same as the computer name.	`CitrixWorkspaceApp.exe ENABLE_DYNAMIC_CLIENT_NAME=Yes`
No	Does not allow the client name to be the same as the computer name. Specify a	`CitrixWorkspaceApp.exe ENABLE_DYNAMIC_CLIENT_NAME=No`

ENABLE_DYNAMIC_CLIENT_NAME COMMAND VALUE	DESCRIPTION	EXAMPLE
	value for the `CLIENT_NAME` property.	

Authentication parameters

Include single sign-on

- Command: `/includeSSON`
- Description: 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.
- Example: `CitrixWorkspaceApp.exe /includeSSON`

Starting with Citrix Workspace app for Windows version 2503, the system installs SSON by default in dormant mode. You can enable SSON post-installation using the Group Policy Object (GPO) policy. To enable, navigate to **User Authentication > Local user name and password** and select the **Enable pass-through authentication** checkbox.

> **Note:**
>
> You must reboot the system after updating the GPO policy for the SSON setting to take effect
>
> The `includeSSON` command supports only fresh installation of Citrix Workspace app.

Enable single sign-on

- Command: `ENABLE_SSON`
- Description: Enables single sign-on when the Citrix Workspace app is installed with the `/includeSSON` command. For more information, see Domain pass-through authentication.

The possible values are the following:

ENABLE_SSON COMMAND VALUE	DESCRIPTION	EXAMPLE
Yes (default)	Indicates that single sign-on is enabled.	`CitrixWorkspaceApp.exe ENABLE_SSON=Yes`
No	Indicates that a single sign-on is disabled.	`CitrixWorkspaceApp.exe ENABLE_SSON=No`

Uninstall Citrix Workspace app

Uninstall using Windows-based uninstaller

You can uninstall Citrix Workspace app for Windows from the **Control Panel**. For more information, see the Uninstall Citrix Workspace app for Windows section.

Note:

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

Uninstall using the command-line interface

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

```
CitrixWorkspaceApp.exe /uninstall
```

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

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

Note:

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

Troubleshooting

Error codes

- For installer related error codes, see MsiExec.exe and InstMsi.exe error messages.
- For system related error codes, see System error codes.

Installer log location

By default, the installer logs are located at the following location:

	INSTALLATION LOG FOLDER	INSTALLATION TYPE
Administrator	For 64-bit: C:\Program Files (x86)\Citrix\Logs and for 32-bit: C:\Program Files\Citrix\ICA Client	Per-system installation
User	%USERPROFILE% \AppData\Local\Citrix\Logs	Per-user installation

Note:

Starting with Citrix Workspace app for Windows 2311.1 version, the `TrolleyExpress` is replaced with `CWAInstaller-<date and timestamp>`. For example, the log is recorded at `C:\Program Files (x86)\Citrix\Logs\CTXWorkspaceInstallLogs-20231225-093441`.

Reset Citrix Workspace app

Resetting Citrix Workspace app restores the default settings.

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

- All the configured accounts and stores.
- Apps delivered by the self-service plug-in, their icons, and registry keys.
- File type associations created by the self-service plug-in.
- Cached files and saved passwords.

- Per-user registry settings.
- Per-machine installations, and their registry settings.
- Citrix Gateway registry settings for Citrix Workspace app.

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

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

For silent reset, use the following command:

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

Note:

Use uppercase U in the parameter.

Resetting Citrix Workspace app does not impact the following:

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

Deploy

You can deploy Citrix Workspace app using one of the following methods:

- Use Active Directory and sample startup scripts to deploy the Citrix Workspace app for Windows. For information about Active Directory, see Using Active Directory and sample scripts.
- When users open their store in a web browser, it can prompt the user to install the Citrix Workspace app for Windows. For more information, see From a store website in a web browser.

- Use an Electronic Software Distribution (ESD) tool like the Microsoft System Center Configuration Manager. For more information, see Using System Center Configuration Manager.
- Use Microsoft Endpoint Manager (Intune). For more information, see Deploy Citrix Workspace app in Microsoft Endpoint Manager (Intune).

Using Active Directory and sample scripts

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

To use the scripts with Active Directory:

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

For information on creating OU in an Azure Active Directory, see Create an Organizational Unit (OU) in an Azure Active Directory Domain Services managed domain.

Edit scripts

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

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

Scripts

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

DEPLOYMENT TYPE	TO DEPLOY	TO REMOVE
Per-computer	`CheckAndDeployWorkspacePerMachineStartupScript.bat`	`CheckAndRemoveWorkspacePerMachineStartupScript.bat`
Per-user	`CheckAndDeployWorkspacePerUserLogonScript.bat`	`CheckAndRemoveWorkspacePerUserLogonScript.bat`

To add the startup scripts:

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

To deploy Citrix Workspace app for Windows:

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

To remove Citrix Workspace app for Windows:

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

From a store website in a web browser

By default, when a user first opens a store in their web browser, it prompts the user to download and install Citrix Workspace app from Citrix's website. Users can manually add the store to Citrix Workspace app, or they can continue in their web browser and only use Citrix Workspace app as the HDX client.

You can configure:

- Whether users are given the option to download and install Citrix Workspace app.
- The location of the installer.
- Whether users are required to use Citrix Workspace app to access the store, or whether they can continue in their web browser.

To configure StoreFront, see Citrix Workspace app deployment.

To configure Citrix Workspace, see Customize store access.

Using System Center Configuration Manager

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

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

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

Adding Citrix Workspace app to the SCCM deployment

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

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

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

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

   The Create Deployment Type wizard appears.

7. In the **General** pane: Set the deployment type to Windows Installer (*.msi file), select **Manually specify the deployment type information**, and click **Next**.
8. In the **General Information** pane: Specify deployment type details (For example: Workspace Deployment) and click **Next**.
9. In the **Content** pane:

   a. Provide the path where the Citrix Workspace app setup file is present. For example: Tools on SCCM server.

   b. Specify **Installation program** as one of the following:

   - `CitrixWorkspaceApp.exe /silent` for default silent installation.
   - `CitrixWorkspaceApp.exe /silent /includeSSON` to enable domain pass-through.
   - `CitrixWorkspaceApp.exe /silent SELFSERVICEMODE=false` to install Citrix Workspace app in non-Self Service Mode.

   c. Specify **Uninstall program** as `CitrixWorkspaceApp.exe /silent /uninstall` (to enable uninstallation through SCCM).

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

    - Set **Setting Type** to File System.
    - Under **Specify the file or folder to detect the application**, set the following:
      - **Type** – From the drop-down menu, select **File**.
      - **Path** – `%ProgramFiles(x86)%\Citrix\ICA Client\Receiver\`

- **File or folder name** – `receiver.exe`
- **Property** – From the drop-down menu, select **Version**
- **Operator** - From the drop-down menu, select **Greater than or equal to**
- **Value** - Type version number of the current Citrix Workspace app

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

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

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

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

    A success message appears.

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

Add distribution points

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

   The Distribute Content wizard appears.

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

   The Add Distribution Points dialog appears.

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

In the Completion pane, a success message appears

4. Click **Close**.

Deploy Citrix Workspace app to the software center

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

   The Deploy Software wizard appears.

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

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

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

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

Creating device collections

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

   The **Create Device Collection** wizard appears.

3. In the **General** pane, type the **Name** for the device and click **Browse** to select the limiting collection.

   This determines the scope of devices, which can be one the default **Device Collections** created by SCCM. Click **Next**.

4. In the **Membership Rules** pane, click **Add Rule** for filtering the devices.

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

- In the **Search for Resources** pane, select the **Attribute name** based on the devices you want to filter and provide the Value for Attribute name to select the devices.

5. Click **Next**. In the Select Resources pane, select the devices that are required to be part of the device collection.

   In the Completion pane, a success message appears.

6. Click **Close**.
7. In the Membership rules pane, a new rule is listed under Click Next.
8. In the Completion pane, a success message appears. Click **Close** to complete the **Create Device Collection** wizard.

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

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

Deploy Citrix Workspace™ app in Microsoft Endpoint Manager (Intune)

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

1. Create the following folders:

   - A folder to store all the source files required for the installation, for example, `C:\CitrixWorkspace_Executable`.
   - A folder for the output file. Output files are in `.intunewin` file, for example, `C:\Intune_CitrixWorkspaceApp`.
   - A folder for the Microsoft Win32 Content Prep Tool, for example, `C:\Intune_WinAppTool`. This tool helps to convert the installation files into the `.intunewin` format. You can download the packaging tool from Microsoft-Win32-Content-Prep-Tool.

2. Convert all the source files that are needed for the installation to a `.intunewin` file:

    a. Launch the command prompt and go to the folder, where the Microsoft Win32 Content Prep Tool exists, for example, `C:\Intune_WinAppTool`.

    b. Run the `IntuneWinAppUtil.exe` command.

    c. On the prompt, enter the following information:

    - **Source folder**: `C:\CitrixWorkspace_Executable`
    - **Setup file**: `CitrixWorkspaceApp.exe`
    - **Output folder**: `C:\Intune_CitrixWorkspaceApp` The `.intunewin` file is created.

3. Add the package to Microsoft Endpoint Manager (Intune):

    a. Open the Microsoft Endpoint Manager (Intune) console: `https://endpoint.microsoft.com/#home`.

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

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

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

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

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

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

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

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

    > **Note:**

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

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

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

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

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

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

4. Verify if the deployment is successful:

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

b. Click **Device install status**.

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

Store configuration

Store

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

A **store** aggregates available applications and desktops for a user into a single place. A user can have multiple stores and switch across stores as needed. An admin delivers the store URL that has preconfigured resources and settings. You can access these stores through the Citrix Workspace app.

Types of stores

You can add the following store types in the Citrix Workspace app:

- Local stores
- Cloud stores
- Custom web store

Cloud stores

Cloud stores are hosted by Citrix® StoreFront cloud.

Local stores

Local stores are hosted by StoreFront. Remote users can connect to the store via a Citrix Gateway.

Custom web stores

If you have created your own custom web portal then you can add it to Citrix Workspace app as a custom web store. To use this feature, the admin must add the domain or custom web store to Client app management allowed URLs.

For more information about configuring custom web store URLs for end-users, see Client app management.

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

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

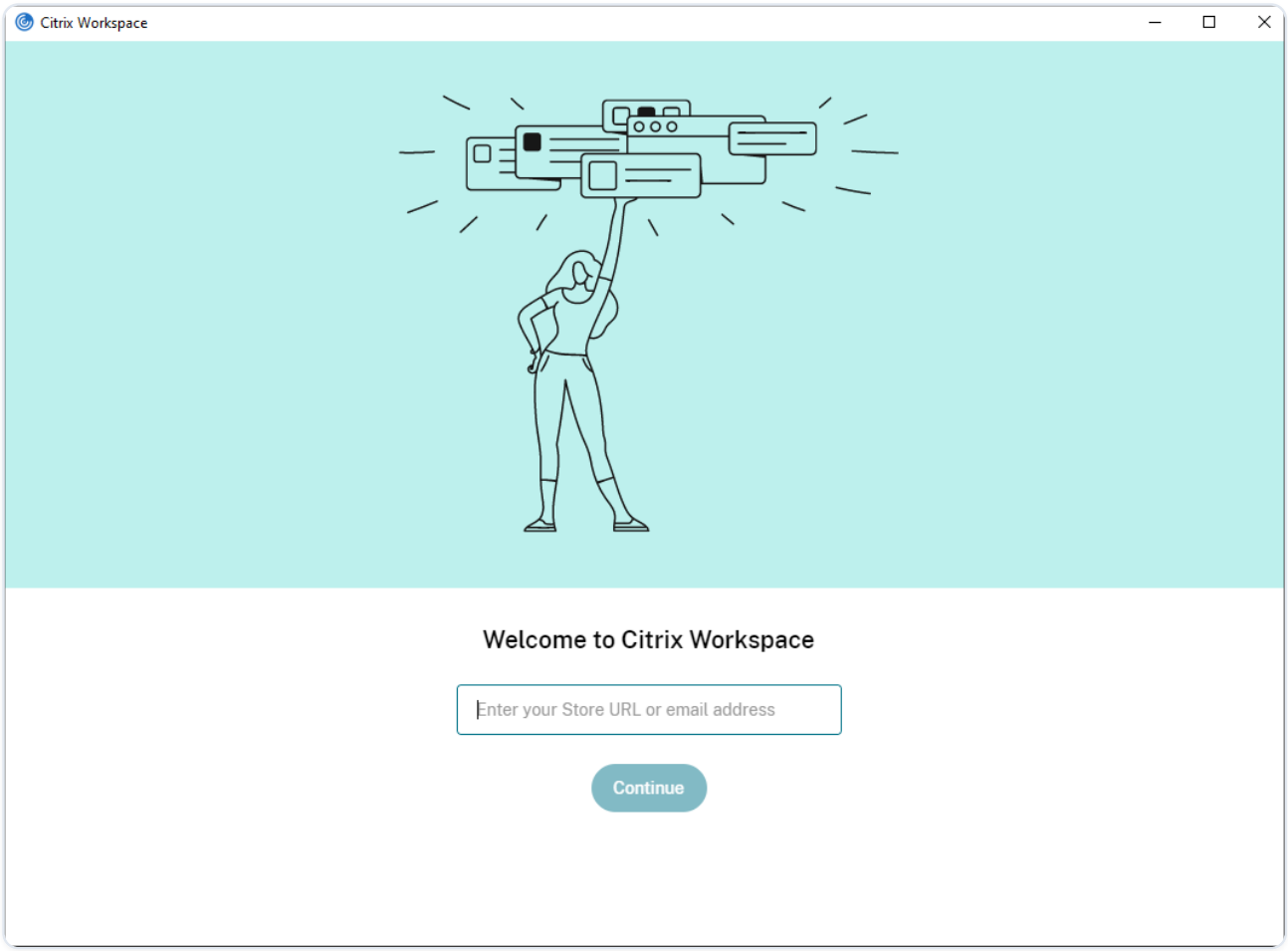
Adding a store to Citrix Workspace app

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

- Providing users with account information to enter manually
- Configuring email-based account discovery
- Adding store through CLI
- Provisioning file
- Using the Group Policy Object administrative template

Provide users with account information to enter manually

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



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

- To connect to a cloud store, provide the cloud store URL.
- If the client can reach the StoreFront deployment without going through a Citrix Gateway, you have the following options:
  - To present a list of all of the non-hidden stores on the server for the user to choose from, provide the base URL. For example: `https://servername.company.com`.
  - To connect to a specific store, provide the Store URL. For example: `https://servername.company.com/Citrix/Store`. Note this is different from the store website URL.
- If the user must connect to StoreFront through Citrix Gateway, you have the following options:
  - To present all stores configured for remote access, provide the Citrix Gateway fully qualified domain name.
  - To connect to a particular store, provide users with the Citrix Gateway fully qualified domain name and the store name in the form:

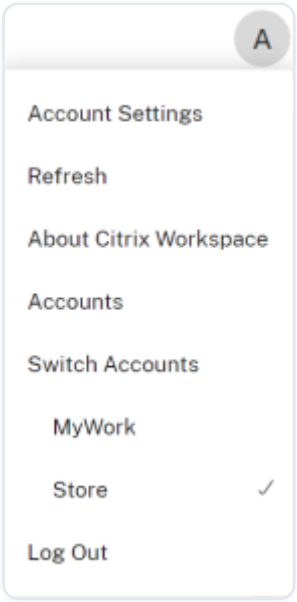
CitrixGatewayFQDN?MyStoreName:

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

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

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

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



On client machines configured for proxy authentication, if the proxy credentials aren't stored in the **Windows Credential Manager**, an authentication prompt appears, asking you to enter the proxy credentials. Citrix Workspace app then saves the proxy server credentials in **Windows Credential Manager**. This results in a seamless login experience because you don't need to manually save your credentials in **Windows Credential Manager** before accessing Citrix Workspace app.

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 reads configuration from Global App Config Service or DNS to find the store URL.

Global App Config Service

You can configure email discovery using the Global App Config Service. For more information, see Configure settings for cloud stores or Configure settings for on-premises stores.

DNS SRV records

For StoreFront stores, you can use DNS SRV records to configure which StoreFront server Citrix Workspace app must use for an email domain.

On your DNS server for your email domain add a **SRV** record with the following properties:

PROPERTY	VALUE
Service	_citrixreceiver
Proto	TCP
Target	The fully qualified domain name (FQDN) and port for your Citrix Gateway appliance (to support both local and remote users) or StoreFront server (to support local users only) in the form *servername.domain:port*.

If your environment includes both internal and external DNS servers, you can add a SRV record specifying the StoreFront server FQDN on your internal DNS server and another record on your external server specifying the Citrix Gateway FQDN. With this configuration, local users are provided with the StoreFront details, while remote users receive Citrix Gateway connection information.

DNS discoverReceiver record

For StoreFront stores, as an alternative to the other methods, you can create a DNS alias to the StoreFront server `discoverReceiver` on the email domain. For example if your email domain is `example.com`, create a DNS alias called `discoverReceiver.example.com`. If no SRV record is found in the specified domain, Citrix Workspace app searches for a machine named "discoverReceiver" to identify a StoreFront server.

If you use this mechanism, ensure that `discoverReceiver` is included as a subject alternate name in the HTTPS certificate for your StoreFront server.

Adding store through CLI

To add a store from the command line, run the following:

```
SelfService.exe -init -createprovider storename https://servername.domain/storepath
```

Provide users with provisioning files

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

You can use StoreFront to create provisioning files that include connection details for accounts. After installing Citrix Workspace app, users simply open the file to configure Citrix Workspace app. For more information, see To export store provisioning files for users in the StoreFront documentation.

If users have access to a store using a web browser, they can go to account settings and download a provisioning file by themselves.

Using the Group Policy Object Administrative Template

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

1. Open the Citrix Workspace app Group Policy Object administrative template by running `gpedit.msc`.
2. Under the **Computer Configuration** node, go to **Administrative Templates** > **Classic Administrative Templates (ADM)** > **Citrix Components** > **Citrix Workspace** > **StoreFront**.
3. Select **Citrix Gateway URL/StoreFront Accounts List**.
4. Select the **Enabled** option and click **Show**. If you enable this policy setting, you can enter a list of StoreFront Accounts and NetScaler Gateway URL.
5. Enter the URL in the **Value** field.
6. Specify the store URL that is used with the Citrix Workspace app:

   `STOREx="storename;http[s]://storeurl/discovery;[On, Off];[storedescription]"`

   Values:

   - `storename` - The name that the user sees for this store.

- `storeurl` - The URL for the store, followed by `/discovery`. If using a Citrix Gateway, enter the gateway URL, followed by `#storename`
- `[On, Off]` - The store enabled state.
- `storedescription` - The description that the user sees for the store, such as HR App store.

For example

```
STORE0="HRStore;https://hr.mycompany.com#Storename;On;HR store"

STORE1="AccountsStore;https://accounts.mycompany.com/discovery;On;Accounts store"
```

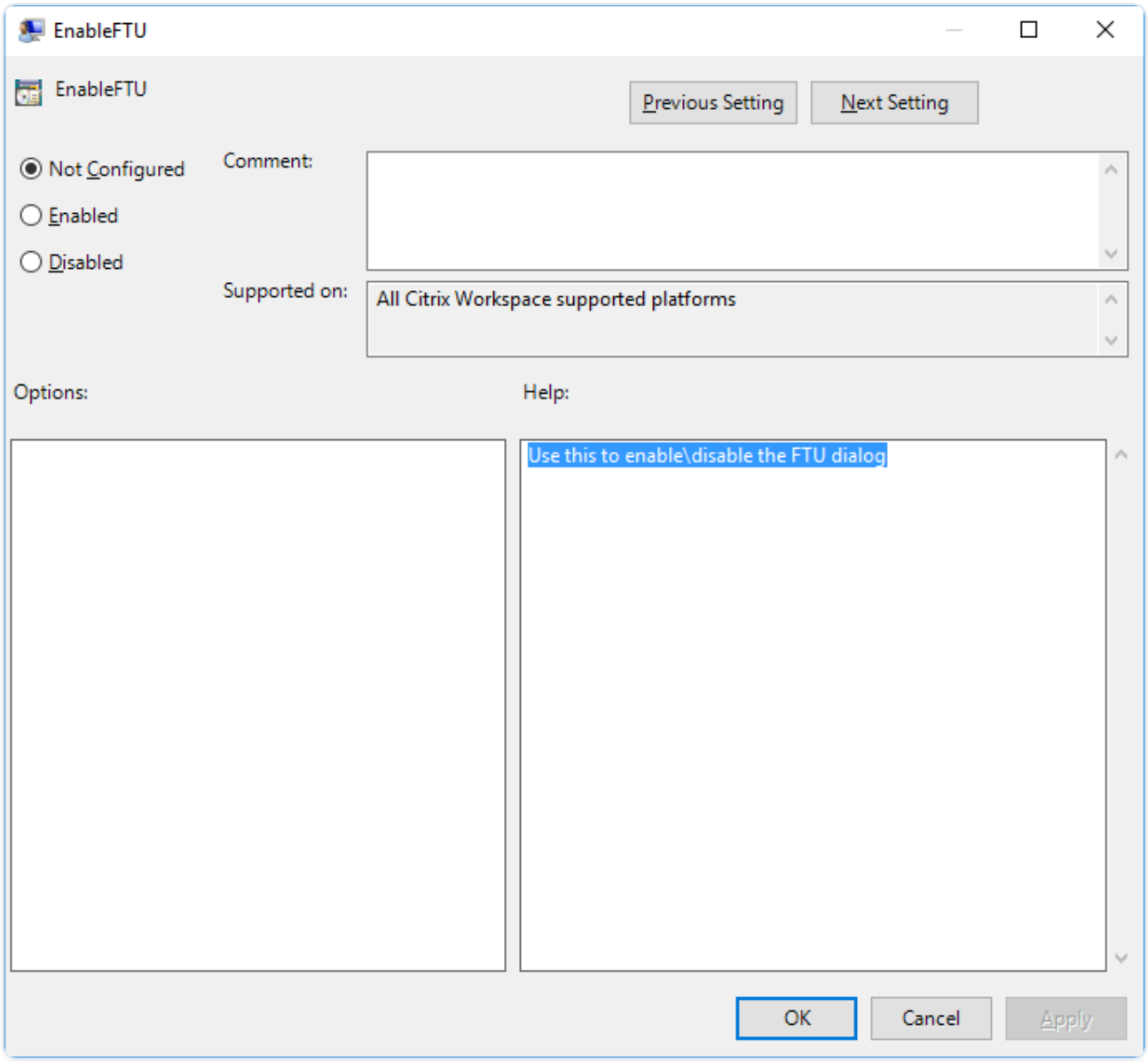
Note:

- The Citrix Gateway store URL must be first in the list (parameter STORE0).
- In a multi-store setup, only one Citrix Gateway store URL configuration is allowed.

Prevent users from adding stores to Citrix Workspace app for Windows

You can choose to prevent users from adding their store to Citrix Workspace app. This could be useful if you prefer users to access their store and launch resources from a web browser, but use Citrix Workspace app to connect to those resources.

To hide the **Add Account** option from the Citrix Workspace app installation wizard, disable **EnableFTUpolicy** under Self-Service node in Local Group Policy Object administrative template as shown below. This is a per-machine setting, hence the behavior is applicable for all users.



Prevent users from using their store from a web browser

You can configure StoreFront and Citrix Workspace so that when users open a store website in their browser, it automatically opens Citrix Workspace app and adds the store.

For more information configuring StoreFront Cloud, see Customize store access.

For more information on configuring StoreFront, see Require use of Citrix Workspace app.

For more information on StoreFront stores accessed through a gateway, see Require Citrix Workspace app when connecting through a gateway.

Domain Name Service name resolution

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

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

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

To disable DNS name resolution for specific user devices:

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

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

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.

StoreFront to StoreFront Cloud Migration

StoreFront to StoreFront Cloud migration enables you to seamlessly migrate your end users from a local store to a cloud store with minimal user interaction.

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

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

To enable the feature, do the following steps:

1. Configure local store to cloud store mapping using client app management. For more information, see Global App Configuration service.
2. Edit the payload in the app config service:

```
{

 "serviceURL": {

"url": "https://storefront.acme.com:443",

"migrationUrl": [

  {

    "url": "https://sampleworkspace.cloud.com:443",

    "storeFrontValidUntil": "2023-05-01"

  }
```

```
 ]
},
"settings": {
"name": "Productivity Apps",
"description": "Provides access StoreFront to Workspace Migration",
"useForAppConfig": true,
"appSettings": {
  "windows": [
    {
      "category": "root",
      "userOverride": false,
      "assignmentPriority": 0,
      "assignedTo": [
        "AllUsersNoAuthentication"
     ],
      "settings": [
      {
       "name": "Hide advanced preferences",
        "value": false
      }
     ]
    }
```

```
    ]
   }
  }
}
```

Note:

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

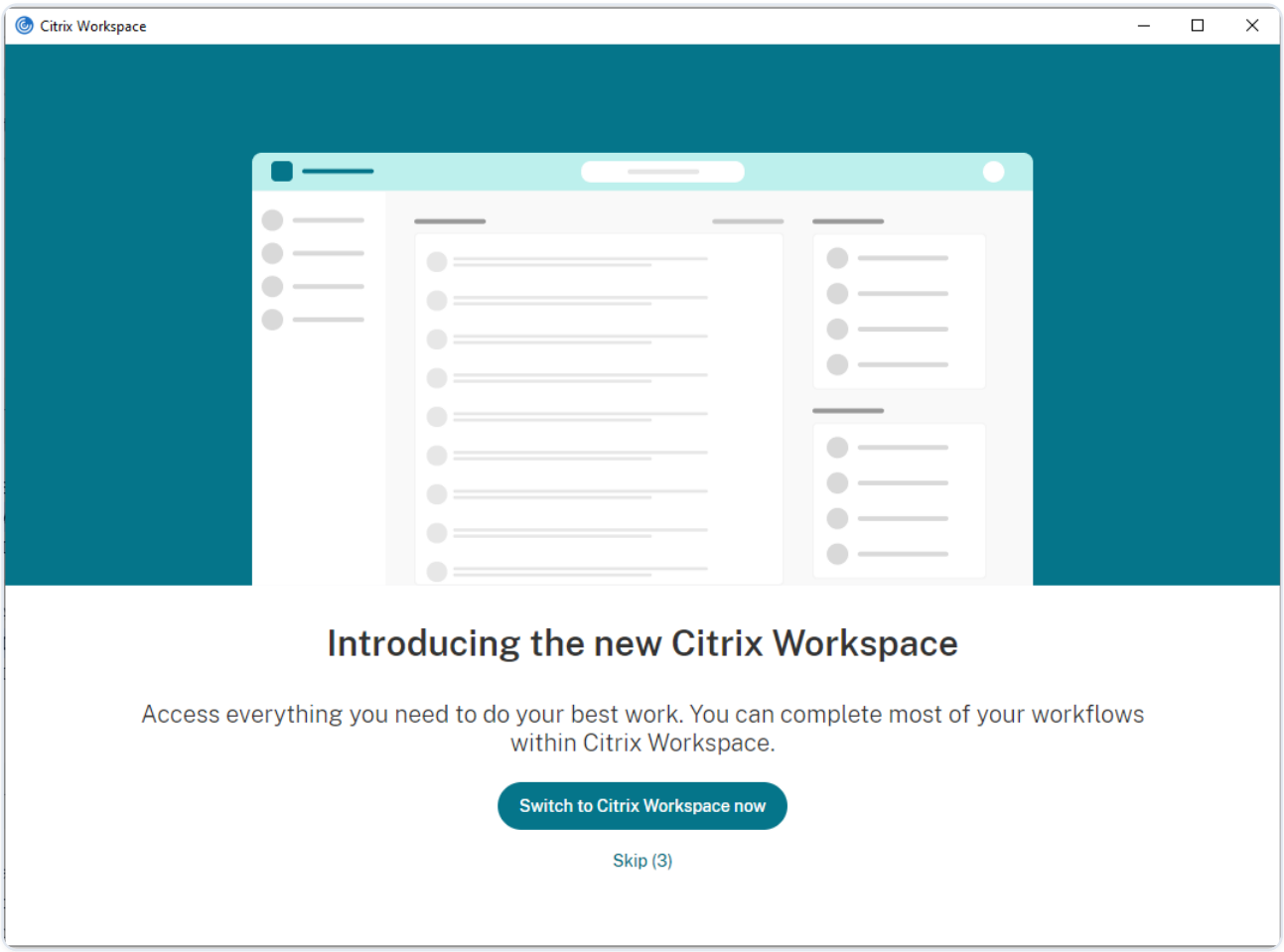
3. Specify the local store URL `storefront.com` as the value for **URL** in the **serviceURL** section.
4. Configure the cloud store URL `xyz.cloud.com` inside the section **migrationUrl**.
5. Use **storeFrontValidUntil** to set the timeline for the removal of the StoreFront store from the Citrix Workspace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

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

     Note:

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

After the app config service settings are pushed, the following screen appears:



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

Support for local app discovery within the Citrix Workspace app

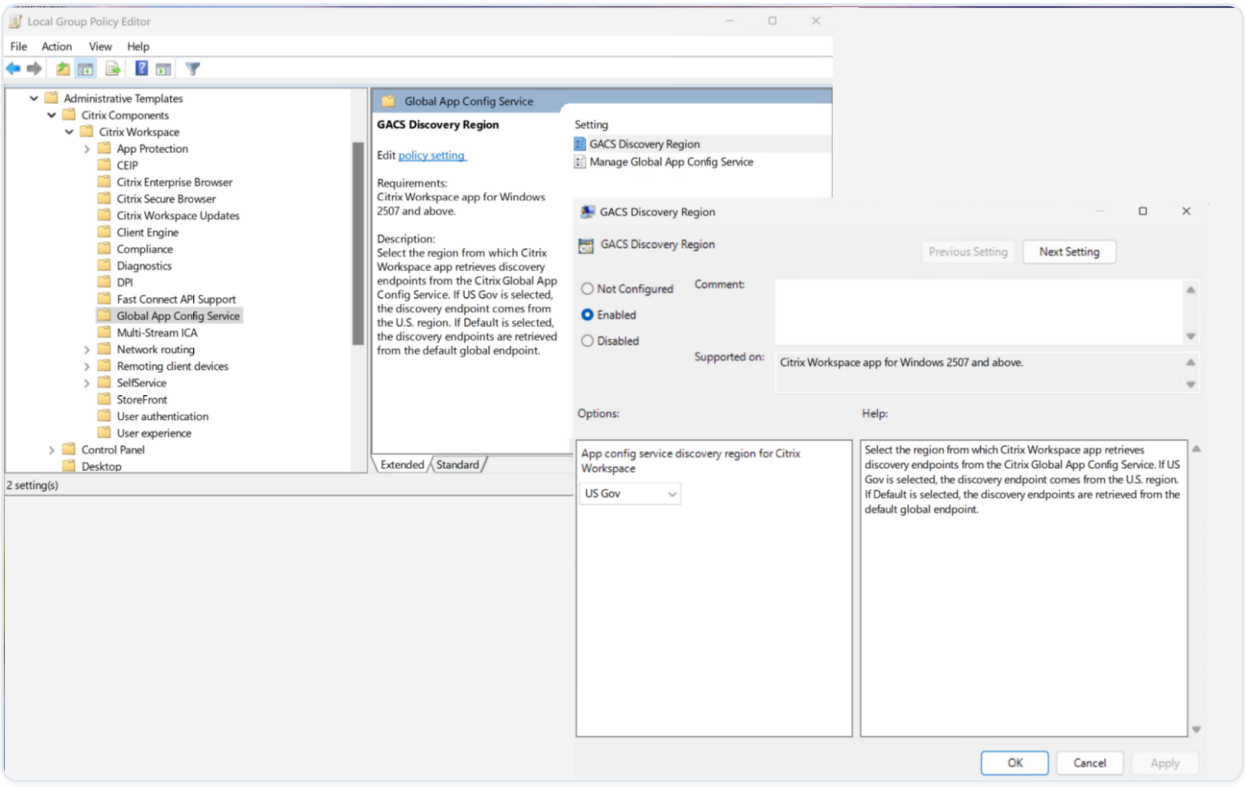
Starting with the 2112.1 release, admins can configure the discovery and enumeration of locally installed apps within the Citrix Workspace app. You can configure this feature by using the Global App Configuration service. For more information, see Global App Configuration service. This feature is ideal for devices that runs in the kiosk mode and for those applications that can't be virtualized within the Citrix Workspace.

Support for GACS claimed URLs for the US Gov region

Starting with version 2507, Citrix Workspace app supports discovery of Global App Config Service (GACS) claimed URLs for the US Gov region alongside commercial cloud deployments.

You can select the region from which Citrix Workspace app retrieves discovery endpoints using the GACS Discovery Region policy setting.

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** > **Global App Config Service**.
3. Select the **GACS Discovery Region** option.



4. Select **Enabled**.
5. Select one of the following options:
   - **US Gov** - Discovery endpoint uses the U.S. region.
   - **Default** - Discovery endpoints uses the default global endpoint.

For more information, see the following:

- Group Policy Object administrative template
- FedRAMP Ready: Citrix Workspace
- Citrix Cloud Government FedRAMP status

Updates and plug-in management

This section describes the following:

- Updates
- Plug-in management

Update

Manual update

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

Automatic update

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

Note:

- If you've configured an SSL intercepting outbound proxy, add an exception to the Workspace auto-update server `https://downloadplugins.citrix.com/` to receive updates from Citrix.
- Auto-update is not available for verisons prior to Citrix Workspace app 2104 and Citrix Workspace app 1912 LTSR CU4.
- Your system must have an internet connection to receive updates.
- By default, Citrix Workspace updates are disabled on the VDA. This includes RDS multi-user server machines, VDI, and Remote PC Access machines.
- Citrix Workspace updates are disabled on machines where Desktop Lock is installed.
- Workspace for web users can't download the StoreFront policy automatically.

- Citrix Workspace updates can be limited to LTSR updates only.
- Citrix HDX RTME for Windows is included in Citrix Workspace Updates. A notification appears when updates to the HDX RTME on both LTSR and current release of the Citrix Workspace app are available.
- Starting with Version 2105, Citrix Workspace Updates log paths are modified. The Workspace Updates logs are present at C:\Program Files (x86)\Citrix\Logs. For information on logging, see Log collection section.
- A non-administrator can update Citrix Workspace app on an admin-installed instance. You can do that by right-clicking the Citrix Workspace app icon in the notification area and selecting **Check for Updates**. The **Check for Updates** option is available on both the user-installed and the admin-installed instances of Citrix Workspace app.
- You can also perform auto-update when Proxy auto-configuration (PAC) and Web Proxy Auto-Discovery Protocol (WPAD) detection is enabled. This is not supported when proxy require credentials for authentication.
- If Non-EDCHE cipher suite is added, Citrix Workspace can't reach Citrix auto-update server and the following error appears during the auto-update:

  Unable to connect to server

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

You can check the current version of Citrix Workspace app installed on your device either through **Advanced Preferences** or query the **DisplayVersion** registry from the `HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\Microsoft\Windows\CurrentVersion\Uninstall\CitrixO` location.

To view the version in the **Advanced Preferences**:

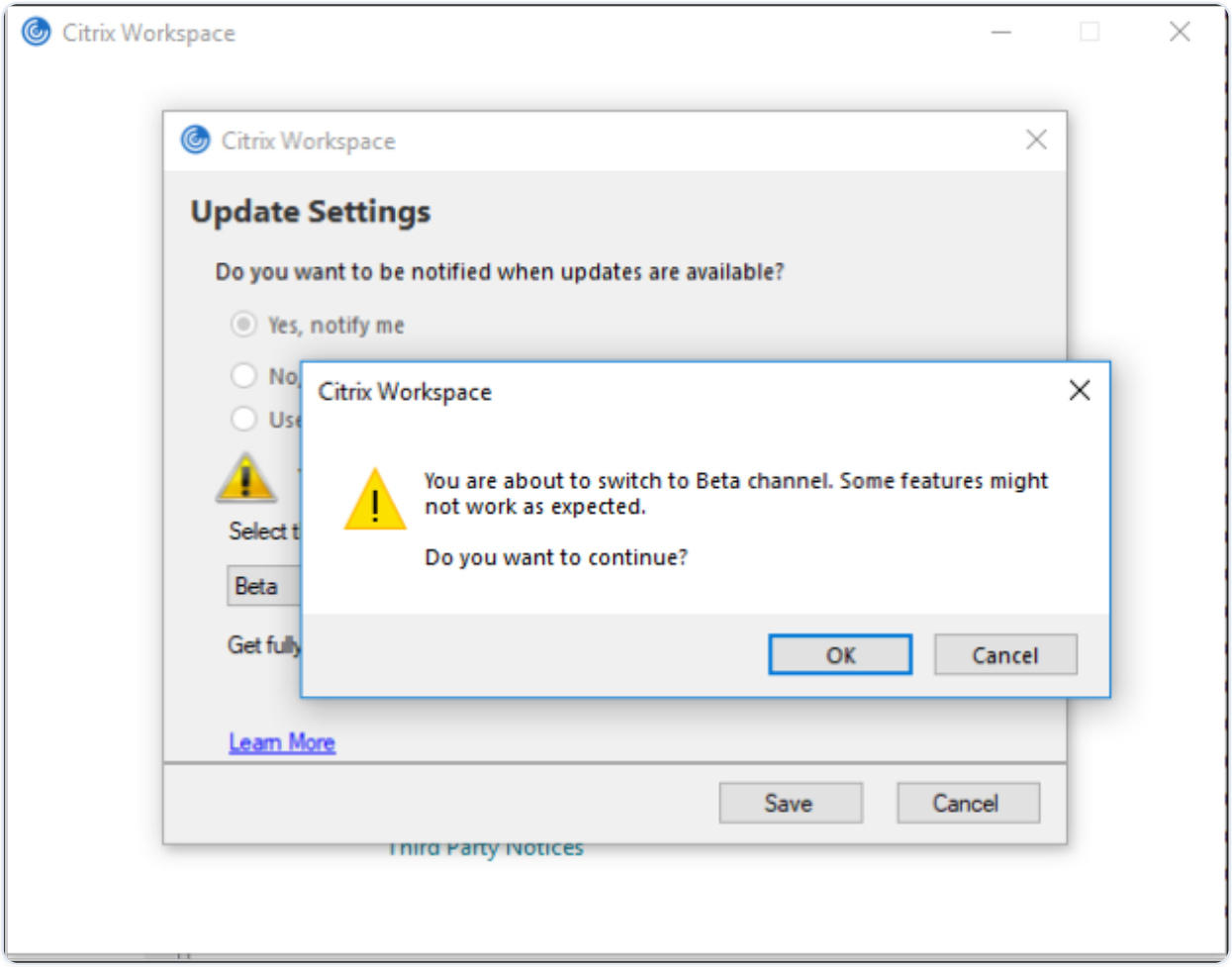
1. Right-click Citrix Workspace app icon from the notification area.
2. Select **Advanced Preferences**.

   Citrix Workspace app version is displayed in the **About** section.

Installing Citrix Workspace app Beta program

You receive an update notification when the Citrix Workspace app is configured for automatic updates. To install the Beta build on your system, do the following steps:

1. Open Citrix Workspace app from the system tray.
2. Navigate to **Advanced Preferences** > **Citrix Workspace updates**.
3. Select **Beta** from the drop-down list, when the Beta build is available, and click **Save**. A notification window appears.



4. Click **OK** to update to Beta build.

To switch from a Beta build to a Release build, do the following steps:

1. Open Citrix Workspace app from the system tray.
2. Navigate to **Advanced Preferences** > **Citrix Workspace updates**.
3. In the **Update Settings** screen, select **Release** from the Update channel drop-down list and click **Save**.

Note:

- If any new updates are available, an auto-update notification appears.

- Beta builds are available for customers to test in their non-production or limited production environments, and to share feedback. Citrix does not accept support cases for beta builds but welcomes feedback for improving them. Citrix might or might not act on feedback based on its severity, criticality, and importance. It's advised that Beta builds aren't deployed in the production environments.

Supporting auto-update of Citrix Workspace app on VDA

Starting with Citrix Workspace app for Windows version 2209, you can enable auto-update feature on VDA. To enable this feature, you must create the following registry value:

On 32-bit machine:

- Registry Key: HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\ICA Client\AutoUpdate
- Registry Value: AllowAutoUpdateOnVDA
- Registry Type: REG_SZ
- Registry Data: True

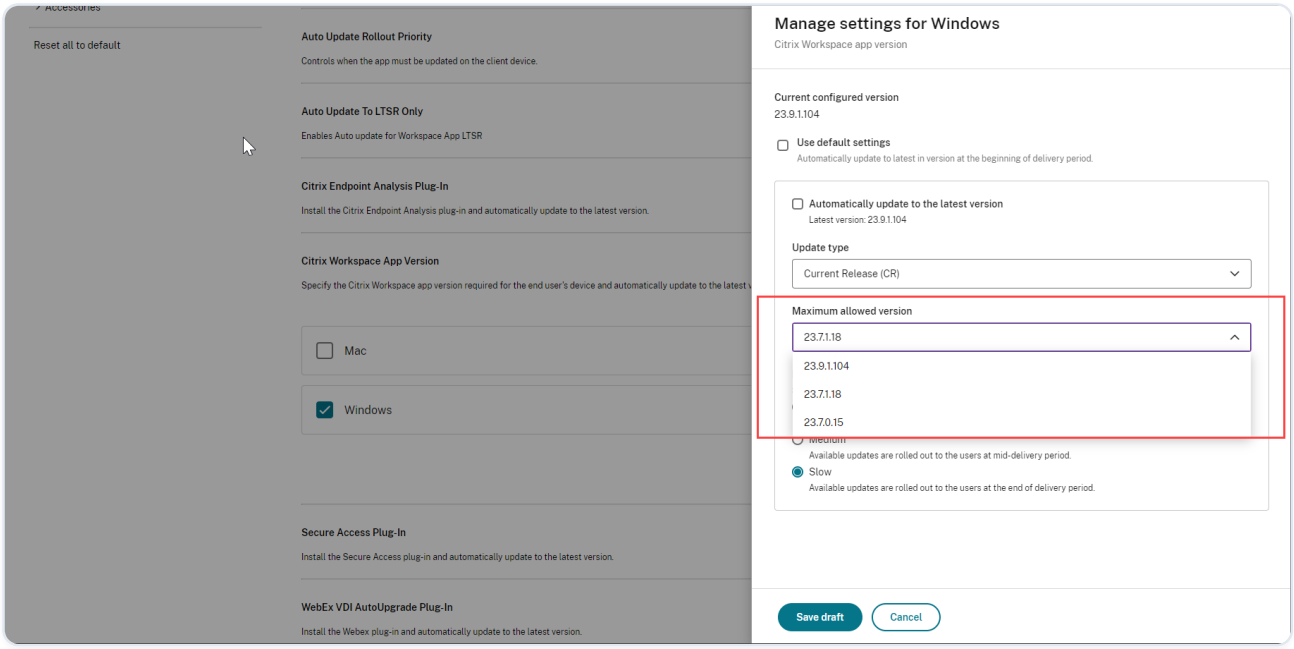
On 64-bit machine:

- Registry Key: HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\Citrix\ICA Client\AutoUpdate
- Registry Value: AllowAutoUpdateOnVDA
- Registry Type: REG_SZ
- Registry Data: True

Auto-update version control

Administrators can now manage the auto-update version for the devices in the organization.

Administrators can control the version by setting the version in the **Maximum allowed version** property in the Global App Config Service.



For more information, see Manage version settings.

> **Note:**
>
> If the administrator hasn't configured the version in the Global App Config Service, Citrix Workspace app is updated to the latest available version by default.

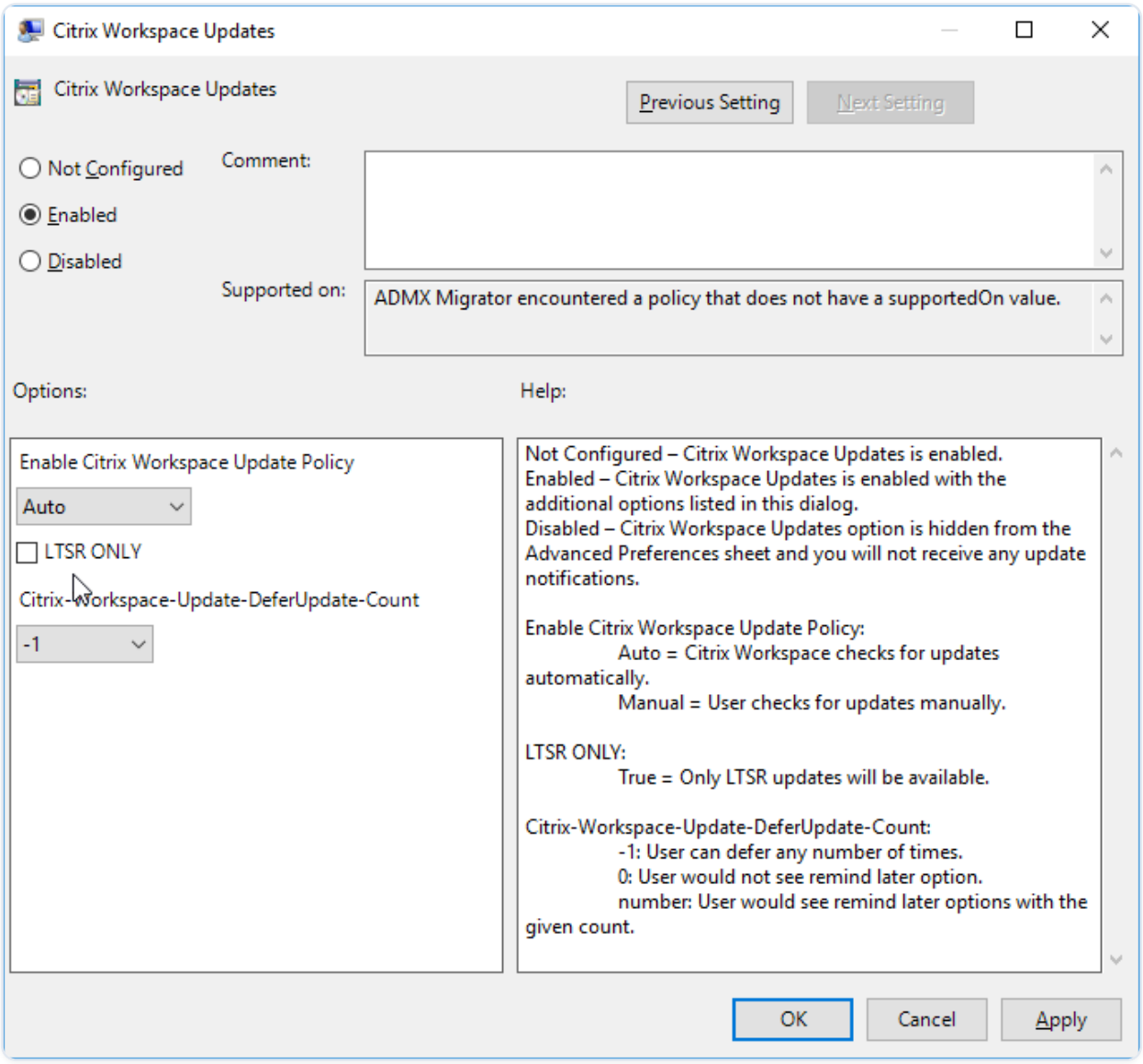
Advanced configuration for automatic updates (Citrix Workspace Updates)

You can configure Citrix Workspace Updates using the following methods:

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

Configure Citrix Workspace Updates using the Group Policy Object administrative template

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



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

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

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

- Auto - You're notified when an update is available (default). This is applicable only for versions prior to Citrix Workspace app 2207. In 2207 or later versions, Citrix Workspace app update is automatic and you aren't notified when an update is available.
- Manual - You aren't notified when an update is available. Check for updates manually.

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

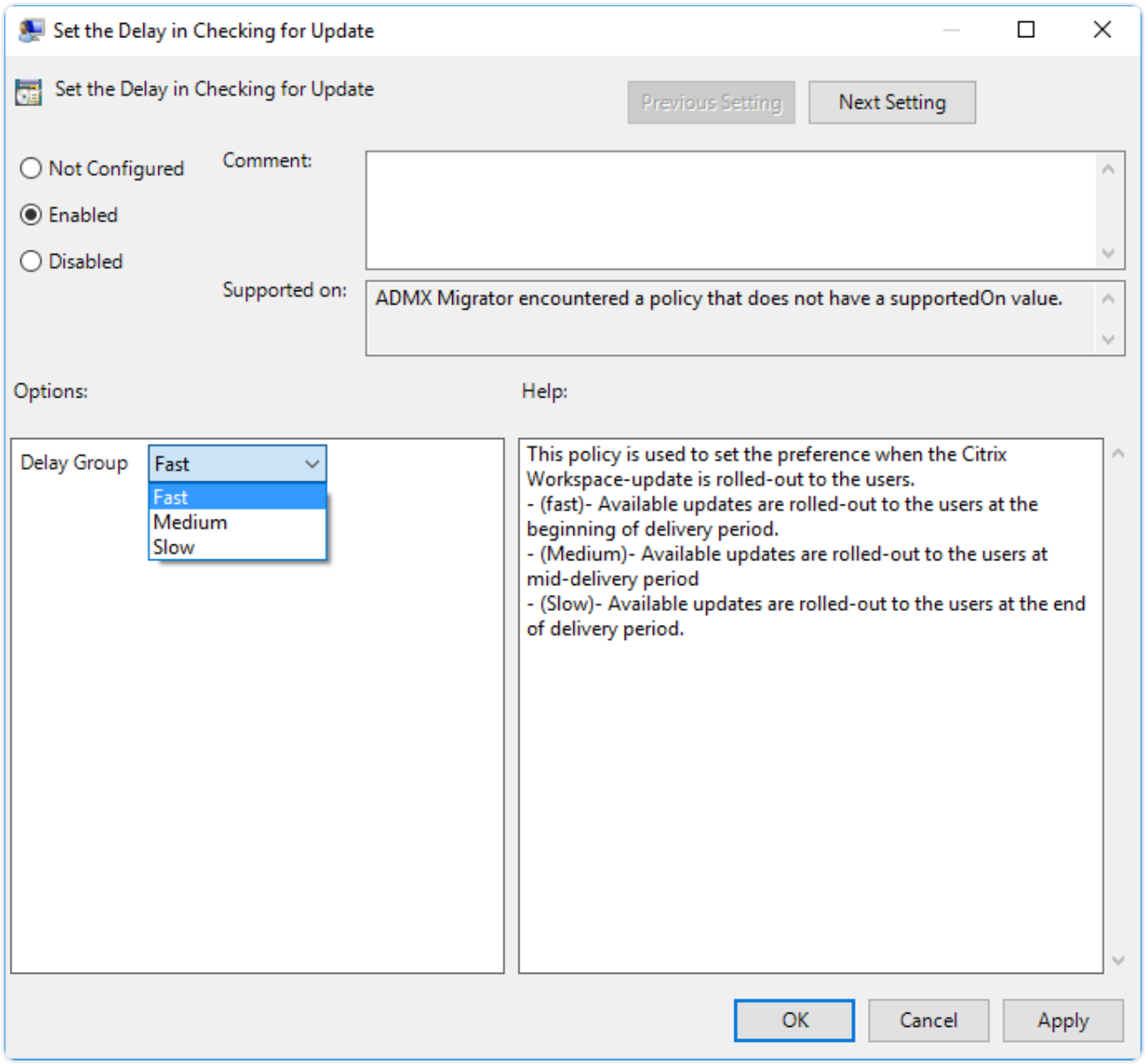
   - If the value is 0, the **Remind Me Later** option doesn't appear. **Update available** prompt is shown on every periodic automatic check for update.
   - If the value is -1, the **Remind Me Later** option appears with the **Update available** prompt. You can defer the update notification any number of times.
   - A value between 1-30 defines the number of times the **Remind Me Later** option with the **Update available** prompt must appear. You can defer the update notification based on the value defined in this field. However, the **Update available** prompt continues to appear but without the **Remind Me Later** option.

> **Note:**
>
> Starting with Citrix Workspace app for Windows version 2207, the auto-update feature is improved and the **Citrix-Workspace-Update-DeferUpdate-Count** field is not required.

Configure the delay in checking for updates

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

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



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

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

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

Configure Citrix Workspace Updates using the command-line interface

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

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

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

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

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

For example,

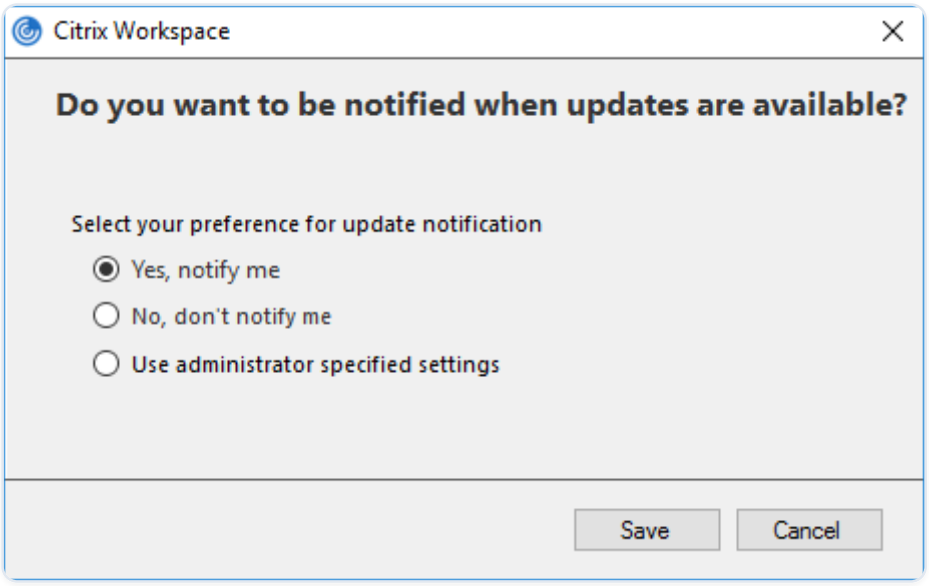
```
CitrixReceiverUpdater.exe /AutoUpdateCheck=auto /AutoUpdateStream=Current /DeferUpdateCount=-1 /AURolloutPriority=fast
```

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

Configure Citrix Workspace Updates using the graphical user interface

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

1. Right-click Citrix Workspace app icon from the notification area.
2. Select **Advanced Preferences** > **Citrix Workspace Updates**.
3. Select one of the following notification preference options:
    - Yes, notify me - You're notified when an update is available for Citrix Workspace app.
    - No, don't notify me - You aren't notified when an update is available for Citrix Workspace app. Check for updates manually.
    - Use administrator specified settings - Uses the settings configured on StoreFront server.



4. Click **Save**.

Note:

- The **Yes, notify me** and the **No, don't notify me** options are applicable only for versions prior to Citrix Workspace app 2207. In 2207 or later versions, the Citrix Workspace app update is automatic and you aren't notified when an update is available. If you select the **No, don't notify me** option, check for updates manually.
- You can hide all or part of the Advanced Preferences sheet available from the Citrix Workspace app icon. For more information, see the Advanced Preferences sheet section.

Configure Citrix Workspace Updates using StoreFront

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

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

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

```
<properties>

      <clear/>
```

```
 </properties>
```

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

```
<account>

    <clear />

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

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

      <annotatedServices>

        <clear />

        <annotatedServiceRecord serviceRef="1__Citrix_F84Store">

          <metadata>

            <plugins>

              <clear />
```

```
            </plugins>

            <trustSettings>

              <clear />

            </trustSettings>

            <properties>

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

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

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

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

                  </properties>
```

```
        </metadata>

      </annotatedServiceRecord>

    </annotatedServices>

    <metadata>

      <plugins>

        <clear />

      </plugins>

      <trustSettings>

        <clear />

      </trustSettings>

      <properties>
```

```
        <clear />


      </properties>


    </metadata>


  </account>
```

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

- **Auto-update-Check:** Indicates that Citrix Workspace app detects an update automatically when available.
  - Auto (default) – Checks and performs updates automatically
  - Manual – updates are only fetched when the user makes a check request from the Citrix Workspace app system tray menu,
  - Disabled – Updates checks are not performed.
- **Auto-update-LTSR-Only:** Indicates that the update is for LTSR only.
  - True – the updater ignores any updates that are not marked as LTSR valid. Only LTSR updates are considered.
  - False (default) - Updater considers only current stream updates.
- **Auto-update-Rollout-Priority:** Indicates the delivery period in which you can receive the update.
  - Fast – updates are rolled-out to the users towards the beginning of the delivery period.
  - Medium – updates are rolled-out towards the middle of the delivery period.
  - Slow– updates are rolled-out towards the end of the delivery period.

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

  > **Note:**
  >
  > This configuration is applicable only for interactive updates and not when the silent auto-update feature is enabled, as the user doesn't get any option to defer the updates.

  - -1: User can defer the auto-update any number of times.
  - 0: User cannot view remind me later option.
  - number: User can view remind later options with the given count.

Define timeframe for automatic update and manage automatic update version and rollout period for Citrix Workspace™ app

The auto-update of Citrix Workspace app is now enhanced with the following features:

- **Define timeframe for automatic update**: Administrators can now schedule automatic updates for Citrix products at any preferred time on their Windows devices. During this specified time, software updates automatically or users receive notifications on available updates.
- **Manage automatic update version and rollout period for Citrix Workspace app**: Administrators can schedule a convenient start date and rollout period for a specific version of Citrix Workspace app during which an automatic update is set to roll out to their end users. This capability allows them to determine the rollout dates, minimizing disruption to end users, and improving the user experience.

> **Note:**
>
> - Starting with the Citrix Workspace app for Windows version 2503, you can enable these features using Group Policy Object (GPO).
> - Starting with the Citrix Workspace app for Windows version 2503.10, you can enable these features using Global App Configuration Service (GACS).

> **Benefits:**

- **Custom rollout period**: Admins can determine the rollout period for their organization, overriding the default period set by Citrix.
- **Scheduled updates**: Admins can specify the hours or time frame during the day to check for and update Citrix Workspace app.
- **Flexible update days**: Admins can choose a specific start date to specify when to download and begin installation updates.

Define timeframe for automatic update

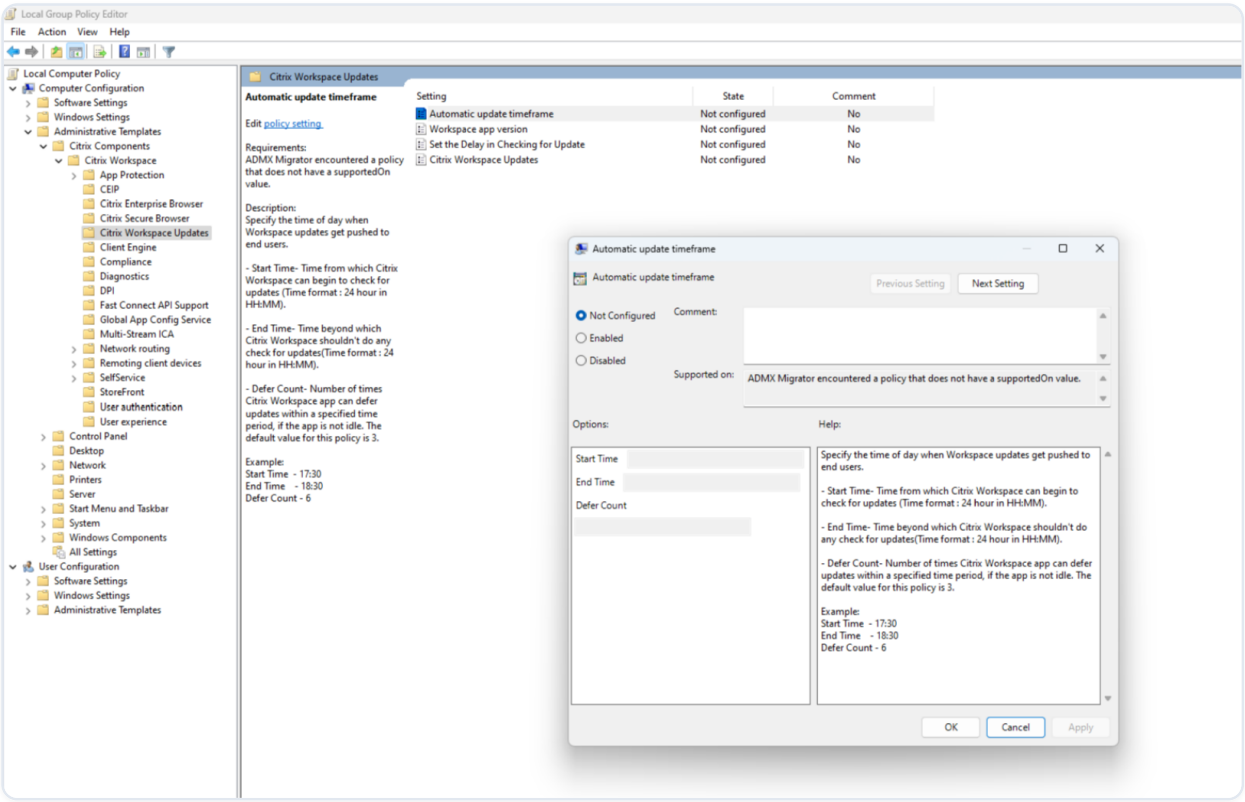
You can define a timeframe for automatic update using Group Policy Object (GPO) and Global App Configuration Service (GACS).

Using GPO:

You can define a timeframe for automatic update using Group Policy Object (GPO). For this, first copy the ADMX and ADML files. For more information, see Group Policy.

Perform the following steps to enable the feature using GPO:

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

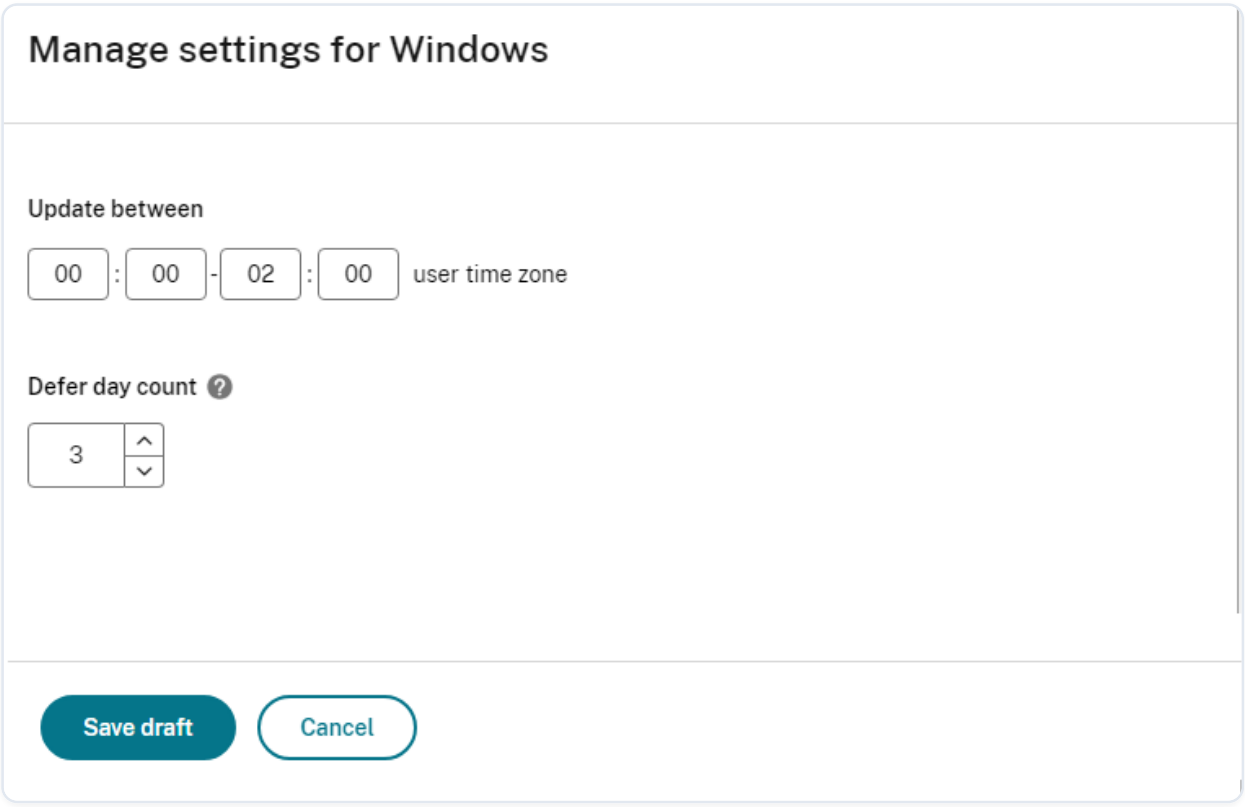


4. Enter the **Start time** from which Citrix Workspace app can begin to check for updates. The time format is 24 hours in HH:MM format. For example: **17:30**.
5. Enter the **End time** after which Citrix Workspace app must not do any check for updates. The time format is 24 hours in HH:MM format. For example: **18:30**.
6. Enter the **Defer count**: The number of times Citrix Workspace app can defer updates within a specified time. When a user runs out of the allocated defer count, the automatic update occurs at any available time.
7. Select the **Enabled** checkbox.
8. Click **OK** and then click **Apply**.

Using GACS:

To enable this feature, do the following:

1. Navigate to **StoreFront Cloud > App Configuration** in Citrix Cloud.
2. Select the required store URL from the list.
3. Navigate to **Configure > Updates and Plug-ins**, and click the **Automatic update timeframe** setting.
4. Select **Windows operating system**, and click **Edit** to define the time window within which an automatic update occurs.



5. In the **Update between** field, add the start time and end time between which you prefer to run the automatic update.

> **Note:**
>
> The difference between start and end time must be at least 1 hour and must be on the same day.

6. In the **Defer day count** field, mention the number of times users can postpone the automatic update. When a user runs out of the allocated defer count, the automatic update occurs during any available time.

For more information, see the Automatic update timeframe in the GACS documentation.

Manage automatic update version and rollout period for Citrix Workspace app

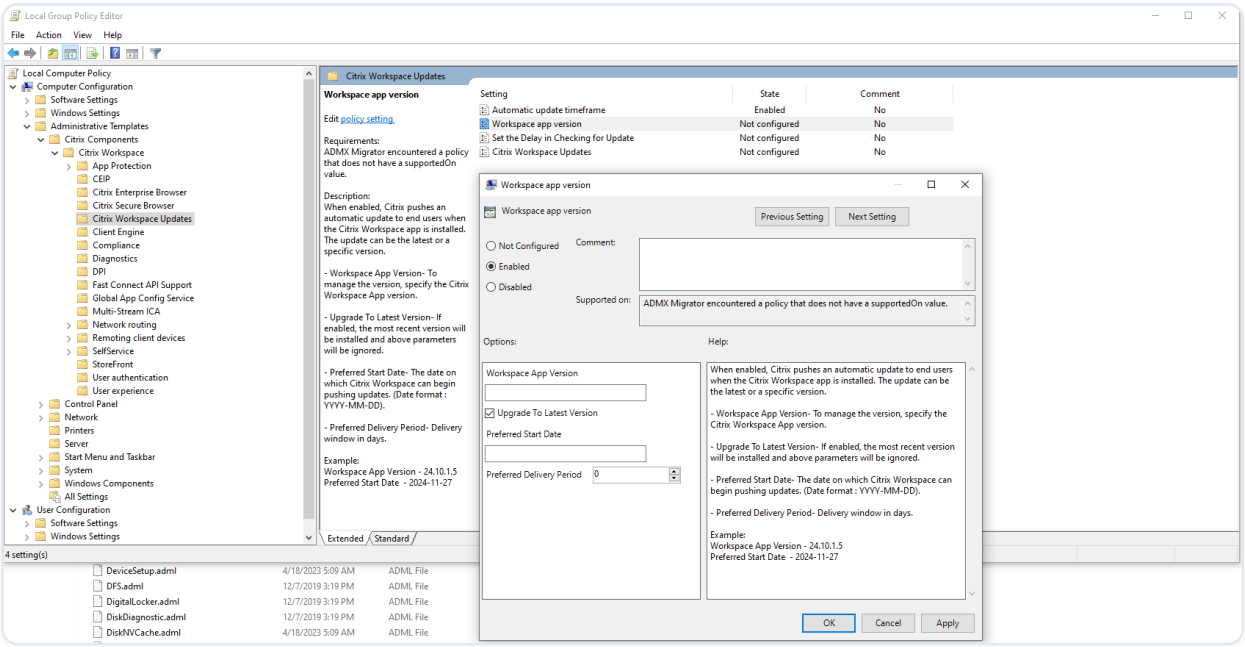
You can manage automatic update version and rollout period for Citrix Workspace app using Group Policy Object (GPO) and Global App Configuration Service (GACS).

Using GPO:

You can manage automatic update version and rollout period for Citrix Workspace app using Group Policy Object (GPO). For this first copy the ADMX and ADML files. For more information, see Group Policy.

Perform the following steps to enable the feature using GPO:

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



4. Enter the required version in the **Workspace App Version** text field. The example format is **24.10.1.5**.

   Or, Select the **Upgrade To Latest Version** checkbox. If you select this checkbox, the most recent version of Citrix Workspace app is installed, and the version added in the **Workspace App Version** text field is ignored.
5. Define the start date on which Citrix Workspace app can begin pushing the updates in the **Preferred Start Date** field. The format is YYYY-MM-DD. For example: **2024-11-27**.
6. Enter the number of days up to which the automatic update rolls out in the **Preferred Delivery Period** field. The automatic update process completes within the specified delivery period.
7. Select the **Enabled** checkbox.
8. Click **OK** and then click **Apply**.

Using GACS:

1. Navigate to **StoreFront Cloud > App Configuration** in Citrix Cloud.
2. Select the required store URL from the list.
3. Navigate to **Configure > Updates and Plug-ins**, and click the **Citrix Workspace app version** setting.
4. Select the operating system, and click **Edit** to configure the setting. The **Manage Setting for Windows** screen appears.

Manage settings for Windows

Citrix Workspace app version

Choose how you want to update

- (•) Update to latest version
  Automatically update to the latest version when it becomes available and use a default update schedule
- ( ) Update to Specific Version
  Manually update to a specific version with granular control over the update schedule

App version

Previous configured version: 24.9.0.100

Latest update version : 24.11.0.6711

Update type

Current Release (CR)

Update schedule

Start rollout on: February 3, 2025

Finish rollout by: February 4, 2025

If the delivery period has passed and the user has not updated to the selected version, the automatic update will be carried out silently in the background without user intervention.

Save draft | Cancel

Manage settings for Windows

Citrix Workspace app version

Choose how you want to update

- ○ Update to latest version
  Automatically update to the latest version when it becomes available and use a default update schedule
- ◉ Update to Specific Version
  Manually update to a specific version with granular control over the update schedule

App version

Previous configured version: 24.9.0.100

Latest update version : 24.11.0.6711

Update type

Current Release (CR)

Version

24.9.0.100

Update schedule

Finish rollout by: February 28, 2025

If the delivery period has passed and the user has not updated to the selected version, the automatic update will be carried out silently in the background without user intervention.

Roll out start date

January 29, 2025

Delivery period

30 days

Save draft | Cancel

5. Select one of the following from the **Choose how you want to update** section:
    - **Update to latest version**: Select this option to automatically update to the latest version when it becomes available and use a default update schedule.
    - **Update to specific version**: Select this option to manually update to a specific version with granular control over the update schedule.
6. If you have selected **Update to latest version**, do the following:
    a. Select the **Update type** from the drop-down list.
    b. Verify the **App version** and update schedules.

    Or,

    If you have selected **Update to specific version**, do the following:

    a. Select the **Update type** from the drop-down list.
    b. Select the **Version** from the drop-down list.
    c. In the **Roll out start date** field, define the start date at which you prefer to start the automatic update of your Citrix Workspace app. Once you set a date, the app doesn't get updated even if a newer version of the app is available.
    d. In the **Delivery period** field, enter the number of days up to which the automatic update rolls out. The automatic update process completes within the specified delivery period.

    The **Update Schedule** displays the rollout finish date based on the date given in the **Roll out start date** field and **Delivery period** field.
7. Click **Save draft**.

> **Note:**
>
> Automatic updates occur only after the user signs in to Citrix Workspace app.

For more information, see Citrix Workspace app version in the GACS documentation.

Enable auto-update for active users only

Starting with version 2503, the auto-update feature has been enhanced to trigger only for active users.

A user is considered active if any of the following criteria is met:

- Managed users using Group Policy Object (GPO) template with Citrix Workspace app version control setting enabled.
- GACS users with Citrix Workspace app version control setting enabled.
- The user has signed in to the current version of Citrix Workspace app.
- The user has opened at least a single Citrix Workspace app session for the current version of Citrix Workspace app. This is applicable in the case of accessing Citrix Workspace app using a browser.

If none of these conditions are met, the user is considered inactive, and the auto-update feature is not available.

When a user transitions from inactive to active status, the auto-update resumes.

Plug-in management

Citrix Workspace app for Windows offers Plug-in management capability that makes the Citrix Workspace app a single client app required on the end point to install and manage the following Citrix and its partner's plug-ins:

- Citrix® plug-ins include:
  - End Point Analysis (EPA) plug-in
  - Secure Access plug-in
- Citrix's Partner plug-ins include:
  - Webex VDI AutoUpgrade plug-in
  - Zoom VDI plug-in Management
  - Microsoft Teams VDI Plug-in Management

With this capability, administrators can easily deploy and manage required plug-ins from a single management console.

Plug-in management includes the following steps:

- Administrators must specify the plug-ins required on end users' devices in the Global App Configuration Service. Administrators can select any of the plug-ins listed previously.
- Citrix Workspace app fetches the list of plug-ins from Global App Configuration Service.

- Based on the list fetched from the Global App Configuration service, Citrix Workspace app downloads the plug-in packages through the auto-update service. If the plug-in is not previously installed on the end point, Citrix Workspace app triggers the installation of the plug-in. If the plug-in is already installed, Citrix Workspace app triggers an update to the plug-in (if the version of the downloaded plug-in is higher than the installed version.)

Citrix Workspace app ensures to automatically update the plug-ins whenever an update is available in the future.

Citrix Workspace app automatically signs in to the plug-ins with the Citrix Workspace credentials.

Notes:

- If any of the plug-ins listed previously doesn't exists, the plug-ins are downloaded and installed while adding the store or account for the first time.
- If the store or account and plug-ins exists and the installer contains a higher version, the plug-ins are updated during the auto-update cycle.

The following diagram illustrates the workflow:



Important:

Global App configuration service is required to enable the Plug-in management feature.

- For the cloud stores, Global app configuration service UI can be accessed in the **StoreFront Cloud** section on the Citrix Cloud admin portal. For more information, see Configure Citrix Workspace app.
- To onboard on-premises stores or if customers need to setup Email based discovery for cloud stores, see Global App Configuration service documentation.

You can enable the Plug-in management feature using the Global App Configuration service UI. Use this method to deploy the latest version of the client.

For more information, see Manage plug-ins using Global App Configuration service.

Enable Plug-in management using Client app management

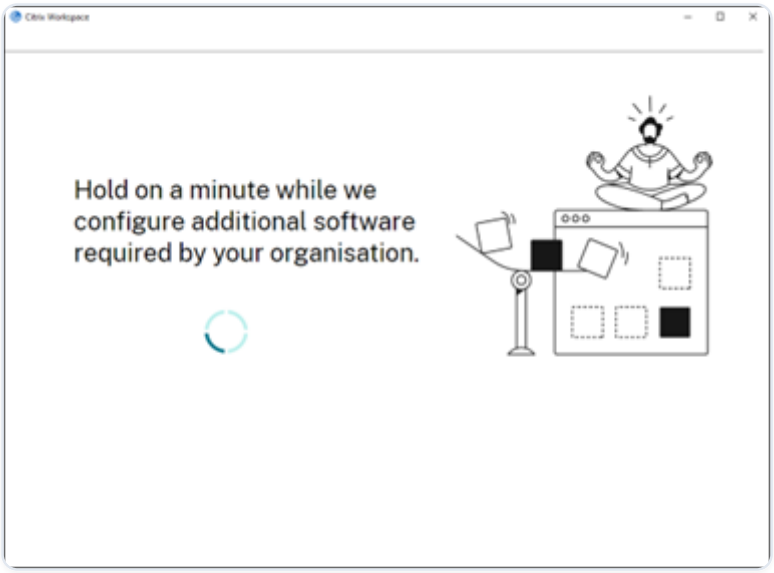
This method is applicable for cloud stores only, plug-ins (EPA / Secure Access, Zoom plug-in, or WebEx plug-in) can be deployed by the admins using the UI.

1. Sign in to Citrix Cloud.
2. From the menu in the top-left of the screen, select **Client app management**. The **Client app management** page appears.
3. Select a profile.
4. Click **Updates and plug-ins** on the left.
5. Select the required plug-in.
6. For **Windows** select **Enabled**.

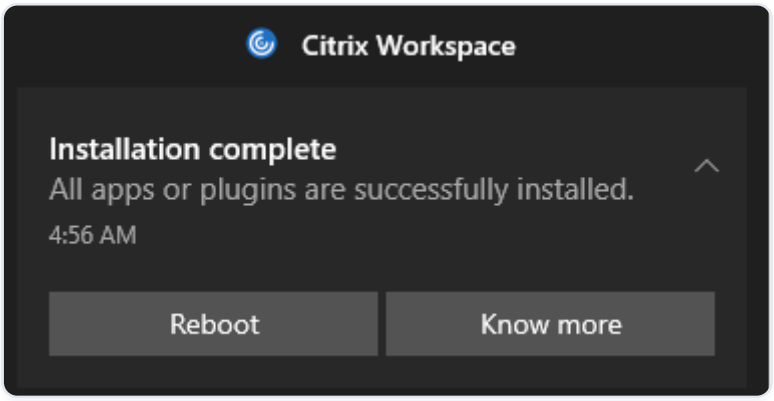
User workflow

1. Download and install the Citrix Workspace app for Windows version 2212.
2. Click **Add Account** at the end of the installation.
3. Add the store/account where the app config settings are onboarded.

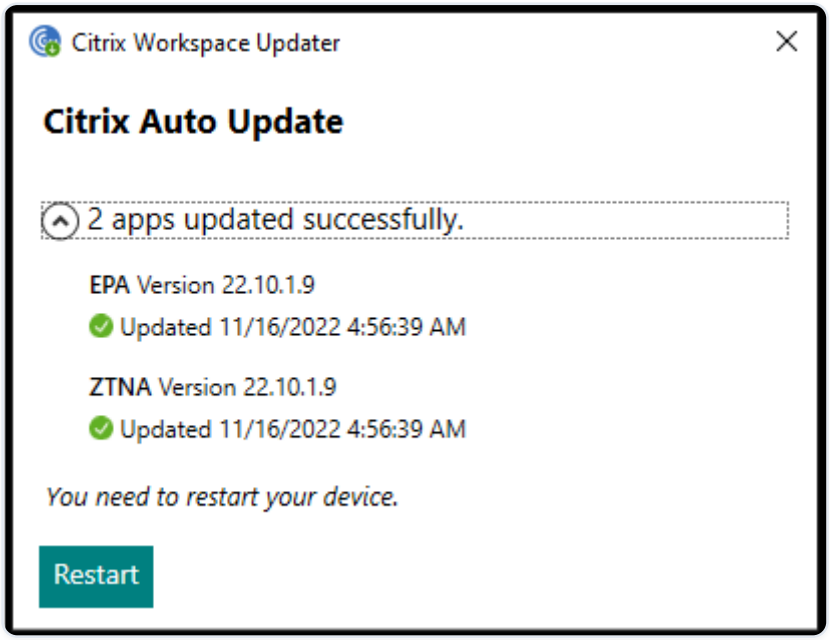
   The following message appears while installing the mandatory plug-ins:



4. When the installation is complete, the following toast notification appears:

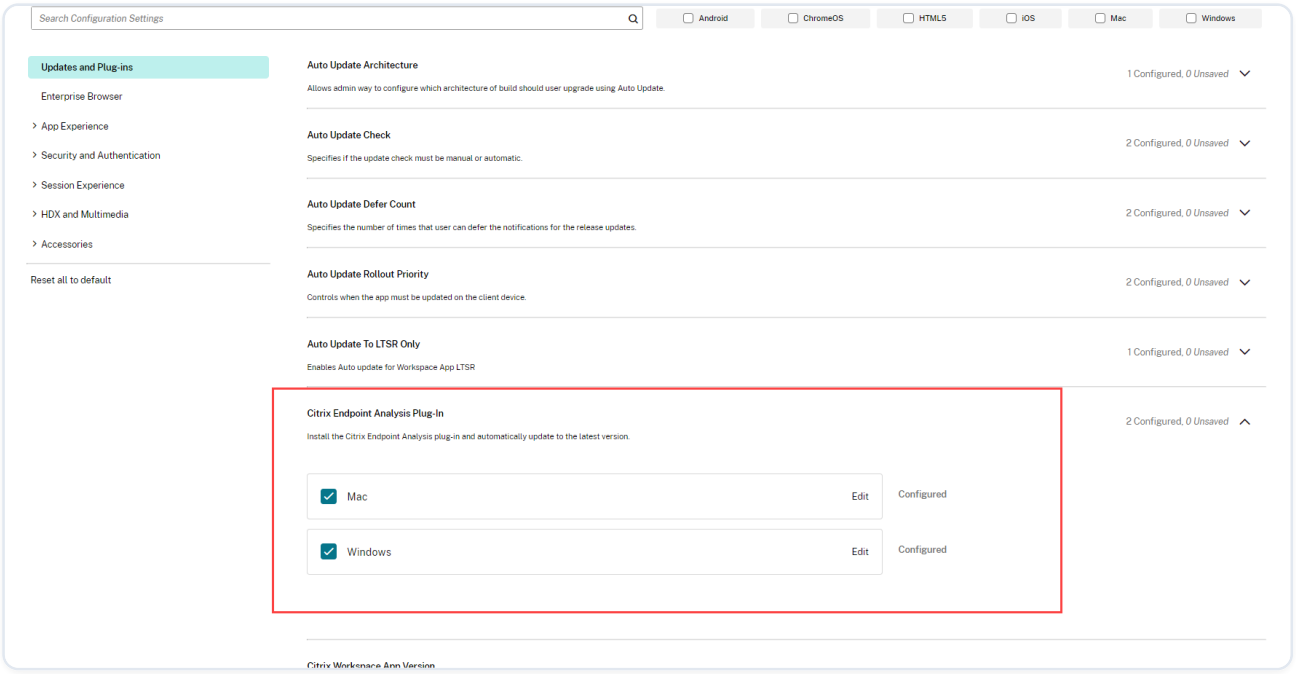


5. Click **Know more** to know the plug-ins installed.



Citrix Endpoint Analysis Plug-in

This setting helps you install and update the Citrix Endpoint Analysis plug-in to the latest version for your end users.



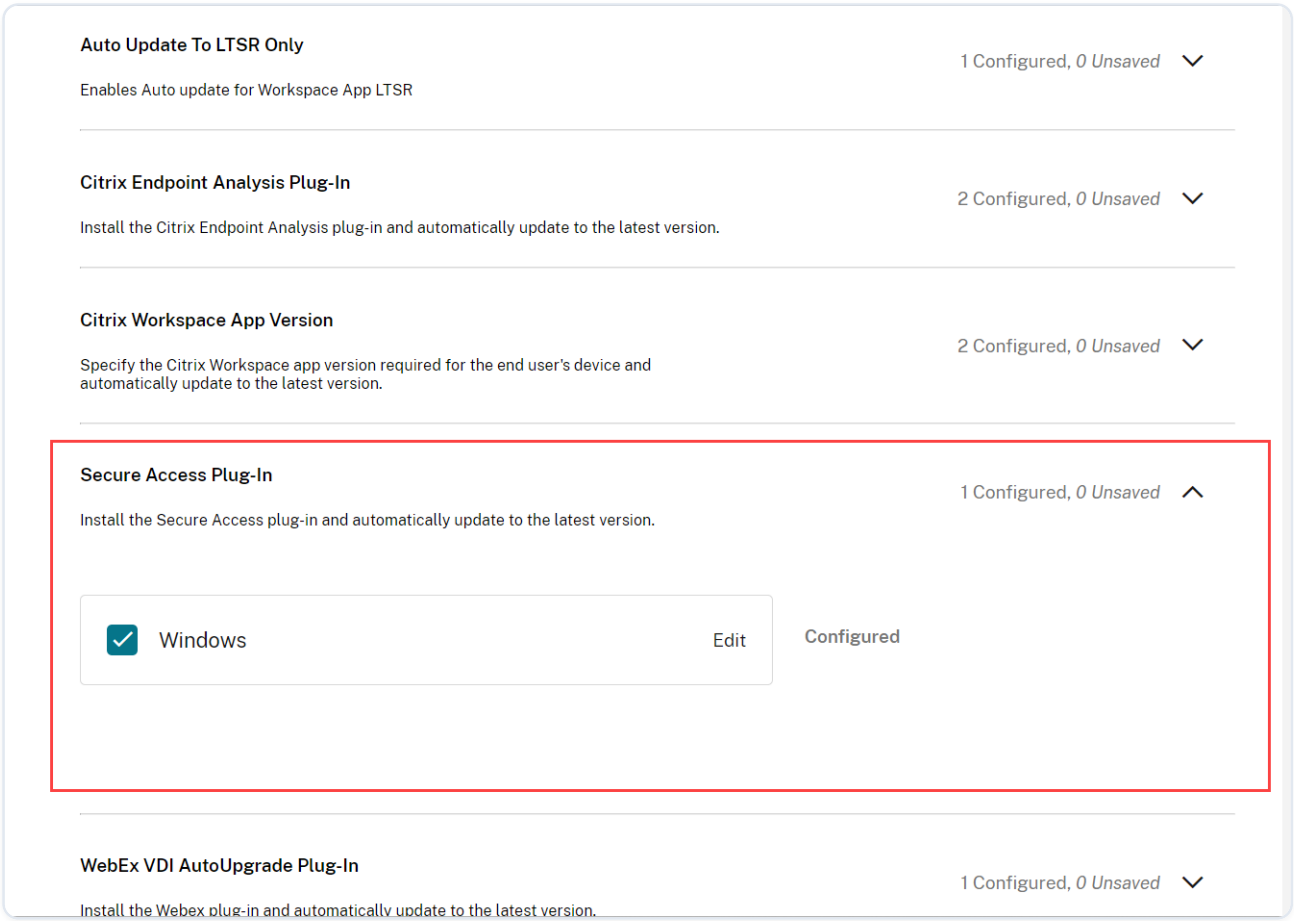
The Citrix Endpoint Analysis plug-in enables you to run device-posture checks on end-user devices. Citrix Device Posture service is a cloud-based solution that helps admins to enforce certain requirements that the end devices must meet to gain access to Citrix DaaS (virtual apps and desktops) or Citrix Secure Private Access™ resources (SaaS, Web apps, TCP, and UDP apps).

For more information, see the Citrix Endpoint Analysis Plug-in documentation.

Citrix Secure Access™ Plug-in

End users can easily access all their sanctioned private apps by installing the Citrix Secure Access plug-in on their client devices.

With the additional support of client-server apps within Citrix Secure Private Access, you can now eliminate the dependency on a traditional VPN solution to provide access to all private apps for remote users.



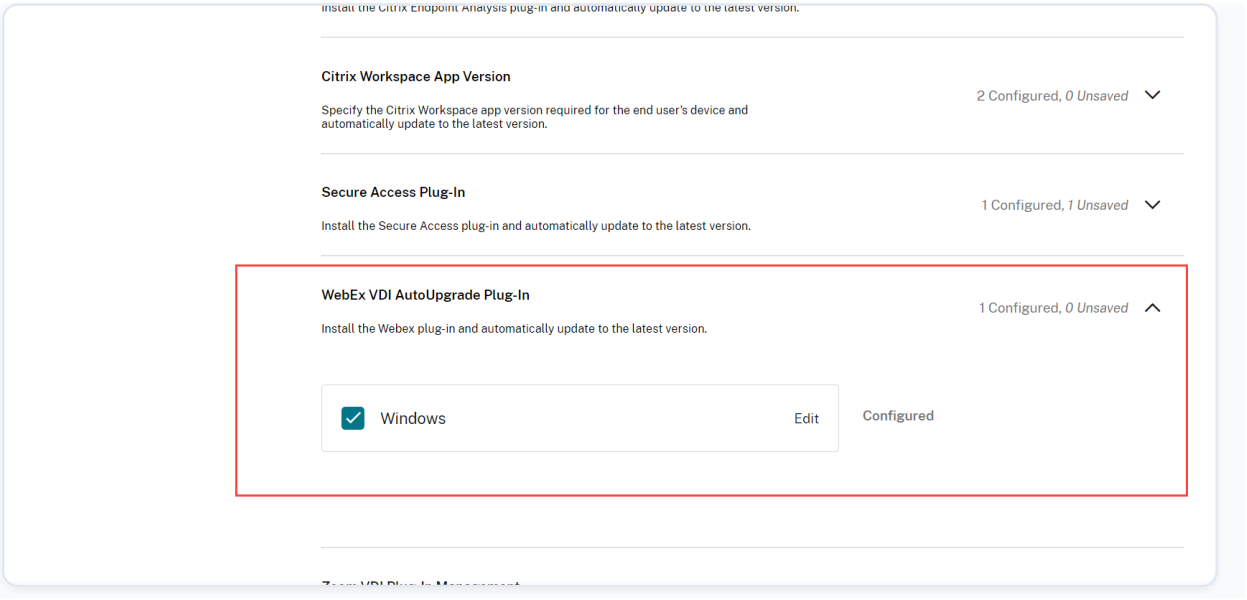
For more information, see the Citrix Secure Access Plug-in documentation.

Plug-in management for WebEx Plug-in

The Webex App VDI solution optimizes the audio and video for calls and meetings. With GACS, you can manage the Webex VDI Plug-in manager. The Webex VDI Plug-in manager, in turn, installs and manages the Webex plug-in installed on the end-user's device.

You can also install Cisco WebEx VDI Plugin as part of Citrix Workspace™ app installation.

> **Important:**
>
> Citrix only manages the installation and update of the Webex VDI Plug-in manager. The Webex plug-in that is installed on the end-user's device is managed by Webex itself.



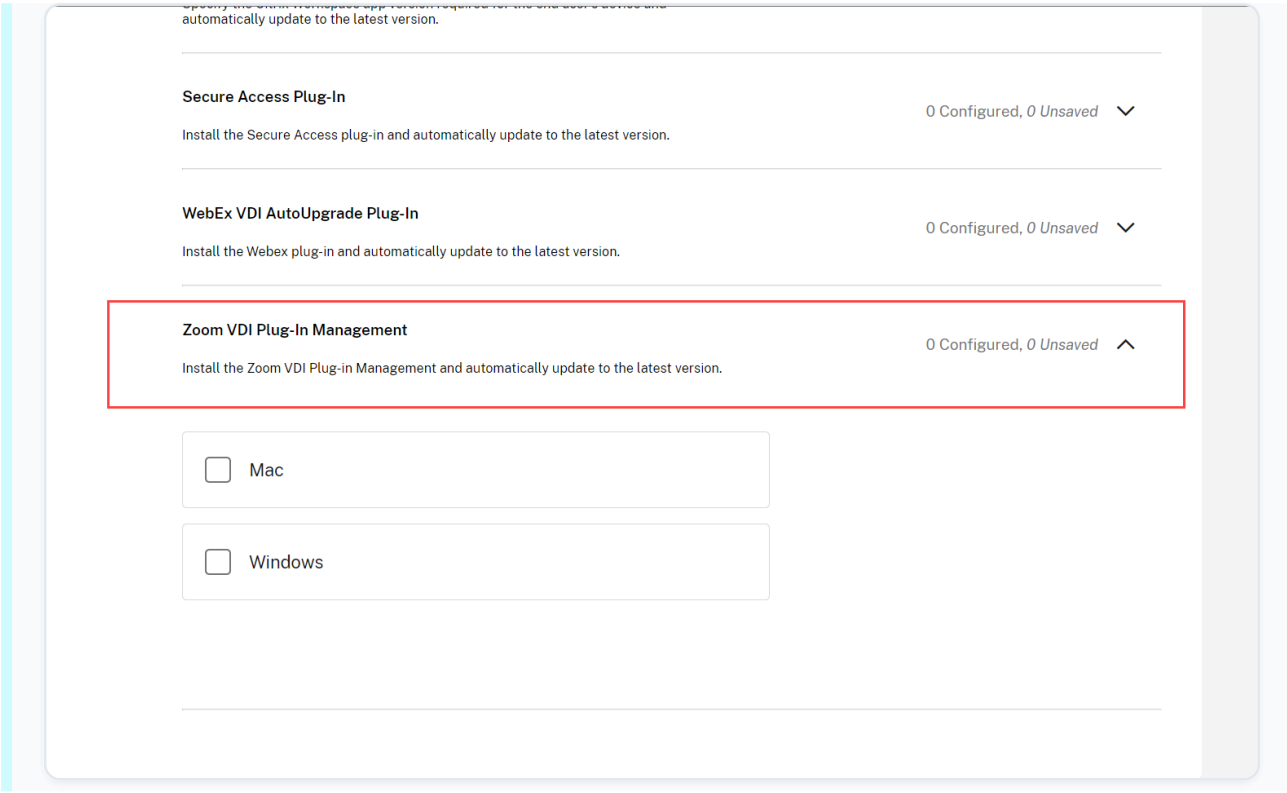
For more information, see the Webex VDI AutoUpgrade Plug-in documentation.

Plug-in management for Zoom plug-in

With GACS, you can manage the Zoom VDI Plug-in manager. The Zoom VDI Plug-in manager, in turn, installs and manages the Zoom plug-in installed on the end-user's device. You can also install Zoom VDI Plugin as part of Citrix Workspace app installation.

Important:

Citrix only manages the installation and update of the Zoom VDI Plug-in manager. The Zoom plug-in that is installed on the end-user's device is managed by Zoom itself.



For more information, see the Zoom VDI Plug-in Management documentation.

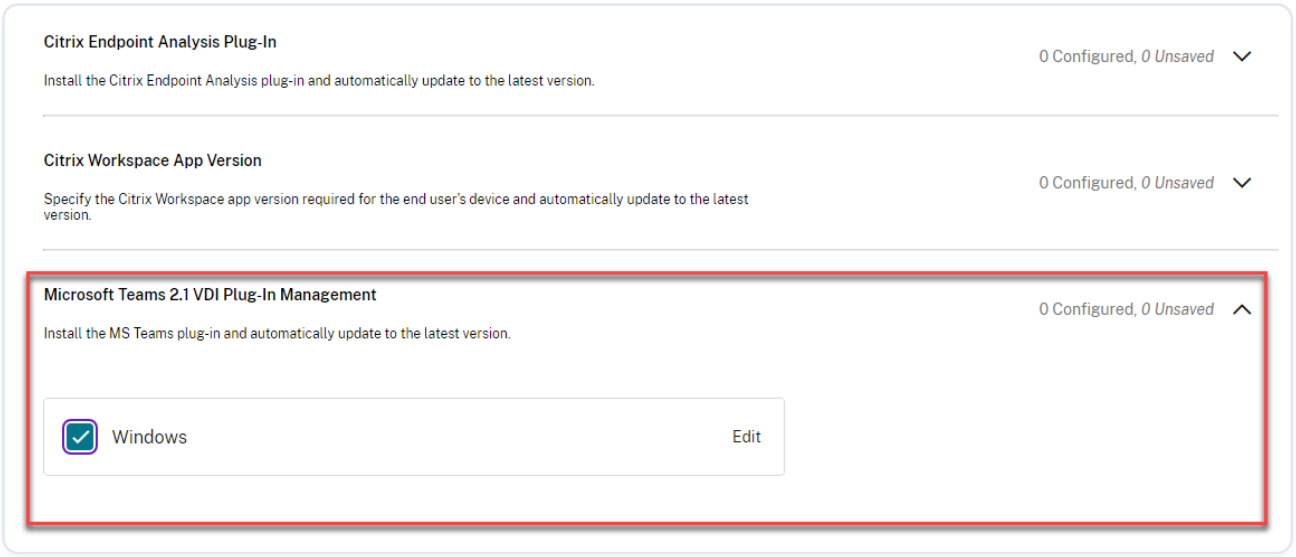
Zoom 64-bit plug-in management support

Zoom has announced that Version 6.2.10 is the last version to support a 32-bit plugin. For more information, see Zoom documentation.

Starting from 2507.1 version onwards, Citrix Workspace app installs the Zoom plug-in management based on the endpoint architecture. If endpoint OS is 64-bit, then Citrix Workspace app installs 64-bit plugin management and keep it updated through auto-update service.

Microsoft Teams VDI Plug-in Management

The Microsoft Teams VDI Plug-in Manager optimizes the audio and video for calls and meetings. With Global App Configuration service, you can manage the installation of Microsoft Teams Plug-in Manager. This Plug-in Manager, in turn, installs and manages the Microsoft Teams Optimization plug-in (VDI 2.0 or Slimcore engine) on the end-user's device.



For more information, see the Microsoft Teams VDI Plug-in Management documentation.

App experience

This section describes the following:

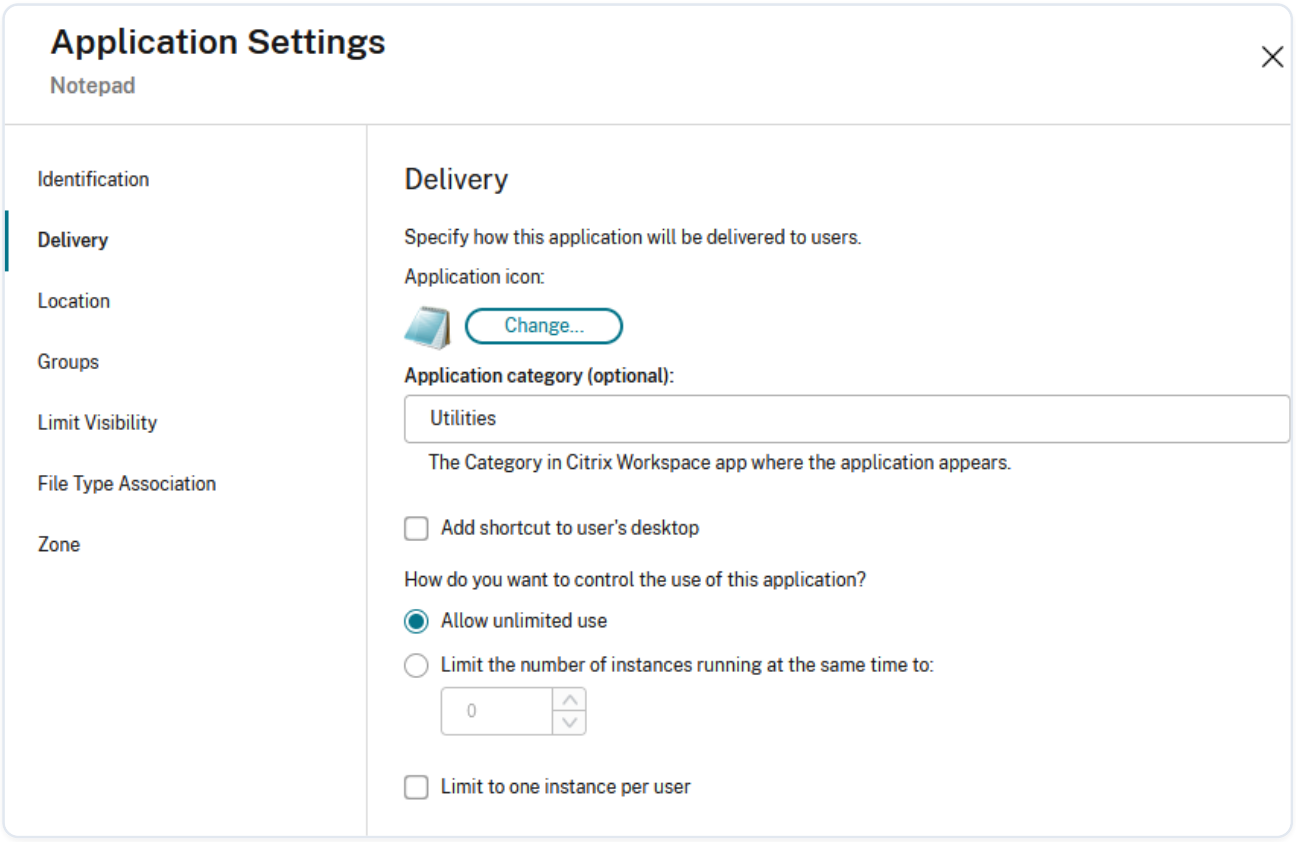
- Application delivery
- Improved virtual apps and desktops launch experience
- App preferences
- SaaS apps
- Data collection and monitoring
- Simplified distribution of uberAgent® on endpoints through Citrix Workspace™ app

Application delivery

Configuring available apps in Studio

To configure in Studio which apps are available to a user, see Applications. In the **Application Settings** screen you can configure the following:

- Select the appropriate icon for the application.
- 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.
- Choose whether to add a shortcut to the user's desktop.
- To make an individual app mandatory, so that it cannot be removed from the Citrix Workspace app **Home** tab, append the string KEYWORDS: Mandatory to the application description.
- To automatically make an application a favorite for all users, append the string KEYWORDS: Auto to the description. When users log on to the store, the application is set as a favorite and added to the Home tab. Users can remove the favorite.



Shortcut only mode

By default when a user installs Citrix Workspace app for Windows, they can open the user interface to view all of their apps and desktops for that store. In addition, apps are added to the **Start** menu depending on configuration. This is known as the "Self-service" mode.

Alternatively, you can disable user interface. This is known as shortcuts-only mode. Apps and desktops can only be opened from the **Start** menu shortcuts.

By default in shortcuts-only mode, users can configure only one store. The **Account** and **Preferences** options are not available to prevent the user from configuring more stores. The administrator can give a user special privileges to add more than one account using the Group Policy Object template. Administrators can also provide special privileges by manually adding a registry key (HideEditStoresDialog) on the client machine. When the administrator gives a user this privilege, the user has a **Preferences** option in the notification area, where they can add and remove accounts.

There are various ways to configure Citrix Workspace app to use shortcuts-only mode:

Global App Config Service

Yon can disable self-service mode using Global App Configuration service.

During installation

You can disable the self-service user interface during installation, see Install.

Group Policy

You can use Group Policy to configure shortcuts-only mode.

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 enable the user interface. This is the default if the policy is not configured.
    b. Select **Disabled** to hides user interface and use shortcuts-only mode.

Application shortcuts for favorite and mandatory apps

When favorites are enabled for a store, by default all favorite and mandatory apps are added to the user's **Start** menu. As users add and remove favorites they are added and removed from the **Start** menu. When favorites are disabled for a store, all apps are added to the user's **Start** menu and the user does not have an option to remove them. If a user removes a shortcut icon from the desktop, the icon comes back next time Citrix Workspace app starts or when the user selects **Refresh** from the icon in the notification area. You can configure the following:

- Disable creation of **Start** menu shortcuts for mandatory and favorite apps. You can continue to configure applications within Studio to create desktop shortcuts.
- Choose the name of the **Start** menu folder.
- For applications that have categories, you can choose whether applications are grouped into sub-folders matching their category name.
- Create shortcuts on the desktop. You can configure the name of a folder to put the shortcuts into and whether applications are grouped into sub-folders matching their category.
- By default shortcuts remain after you log out of your store or exit Citrix Workspace app. You can choose to remove shortcuts when the user logs off the store exits Citrix Workspace app exits. This is useful when the device is shared by multiple people.
- Choose whether modified apps are automatically reinstalled. When enabled, any changes to the published apps and desktops attributes on the server appear on the client machine. When

disabled, apps and desktop attributes aren't updated. Also, shortcuts aren't restored on refresh if they are deleted on the client. By default, this is enabled.

You can configure these shortcuts using the following mechanisms:

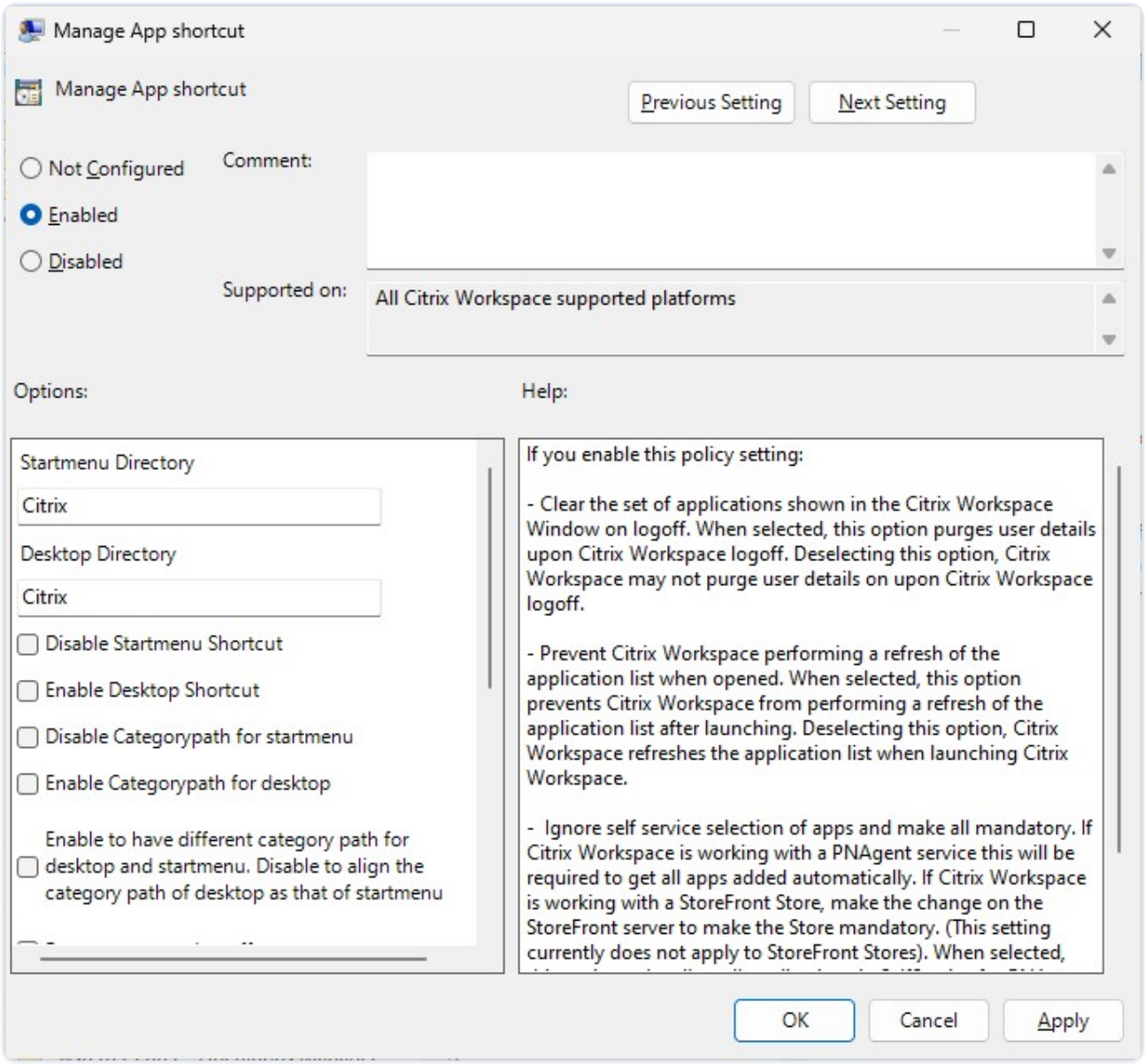
Global App Config Service

In the Global App Configuration service, update the settings under **App Experience** > **Desktop Shortcuts**.

Group Policy

You can use Group Policy to configure shortcuts.

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 App Shortcut** policy.
4. Select the options as required
5. Click **Apply** and **OK**.
6. Restart Citrix Workspace app for the changes to take effect.



StoreFront account settings

You can use StoreFront account settings. You can set the following properties:

PROPERTY NAME	DESCRIPTION	VALUE	DEFAULT
`PutShortcutsOnDesktop`	Put shortcuts on the desktops.	`true` or `false`	`false`
`PutShortcutsInStartMenu`	Put shortcuts in the **Start** menu.	`true` or `false`	`true`
`UseCategoryAsStartMenuPath`	Use the category path in the **Start** menu.	`true` or `false`	`true`

PROPERTY NAME	DESCRIPTION	VALUE	DEFAULT
`StartMenuDir`	Sets a single directory for all shortcuts in the **Start** menu	String value, being the name of the folder into which shortcuts are written.	
`AutoReinstallModifiedApps`	Reinstall modified apps.	`true` or `false`	`true`
`DesktopDir`	Show a single directory for all shortcuts on the desktop.	String value, being the name of the folder into which shortcuts are written	
`DontCreateAddRemoveEntry`	Do not create an entry on the clients 'add/remove programs'.	`true` or `false`	`false`
`SilentlyUninstallRemovedResources`	Remove shortcuts for an application that was previously available from the Store but now is not available.	`true` or `false`	`false`

Windows Registry

You can use the Windows registry to configure shortcuts. Under `HKLM\Software\Wow6432Node\Citrix\Dazzle` add values of type String, with the same value names as used for StoreFront account settings.

During installation

You can configure the directory for the **Start** menu and desktop shortcuts during installation. For more information, see Install.

Support for 32-bit color icons

Citrix Workspace app supports 32-bit high color icons. To provide for seamless applications, it automatically selects the color depth for:

- applications visible in the **Connection Center** dialog,
- the **Start** menu, and
- task bar

Caution

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

To set a preferred depth, you can add a string registry key named `TWIDesiredIconColor` to `HKEY\LOCAL\MACHINE\SOFTWARE\Wow6432Node\Citrix\ICA Client\Engine\Lockdown Profiles\All Regions\Preferences` and set it to the required value. The possible color depths for icons are 4, 8, 16, 24, and 32 bits-per-pixel. The user can select a lower color depth for icons if the network connection is slow.

Reducing enumeration delays or digitally signing application stubs

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

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

This functionality involves several steps:

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

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

- Run `reg add HKEY_CURRENT_MACHINE\Software\Citrix\Dazzle /v ReuseStubs /t REG_SZ /d "true"` or

Alternatively add to HKEY_CURRENT_USER. HKEY_CURRENT_USER has preference over HKEY_LOCAL_MACHINE.

Caution

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

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

1. On a client machine, create stub executables for all apps. To accomplish create stub executables, add all the applications to the machine using Citrix Workspace app. Citrix Workspace app generates the executables.
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 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.
   c. Exit and restart Citrix Workspace app for the changes to take effect.

Launching local applications

In a double-hop scenario (where Citrix Workspace app is running on the VDA that hosts your session), you can control whether Citrix Workspace app launches:

- the local instance of an application installed on the VDA (if available as a local app) or
- a hosted instance of the application.

There are two mechanisms for achieving this. It is recommended that you use vPrefer. Alternatively you can use the Prefer keyword.

vPrefer

vPrefer was introduced with Citrix Workspace app for Windows 4.11 and requires StoreFront Version 3.14 and Citrix Virtual Desktops 7.17 and later.

When you launch the application, Citrix Workspace app reads the resource data present on the StoreFront server and applies the settings based on the **vprefer** flag at the time of enumeration. Citrix Workspace app searches for the application's installation path in the Windows registry of the VDA. If present, launches the local instance of the application. Otherwise, a hosted instance of the application is launched. If you launch an application that is not on the VDA, Citrix Workspace app launches the hosted application. For more information on how StoreFront handled the local launch, see Control of local application launch on published desktops in the Citrix Virtual Apps and Desktops documentation.

If you do not want the local instance of the application to be launched on the VDA, set the **LocalLaunchDisabled** to **True** using the PowerShell on the Delivery Controller. For more information, see the Citrix Virtual Apps and Desktops documentation.

This feature helps to launch applications faster, thereby providing a better user experience. You can configure it by using Group Policy. 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. For an upgrade, the existing settings are retained while importing the latest files.

1. Open the Citrix Workspace app GPO administrative template by running gpedit.msc.
2. Under the **Computer Configuration** node, go to **Administrative Template** \> **Citrix Component** \> **Citrix Workspace** \> **SelfService**.
3. Select the **vPrefer** policy.
4. Select **Enabled**.
5. From the **Allow apps** drop-down list, select one of the following options:

- **Allow all apps**: This option launches the local instance of all apps on the VDA. Citrix Workspace app searches for the installed application, including the native Windows apps such as Notepad, Calculator, WordPad, Command prompt. It then launches the application on the VDA instead of the hosted app.
- **Allow installed apps**: This option launches the local instance of the installed app on the VDA. If the app is not installed on the VDA, it launches the hosted app. By default, **Allow installed apps** is selected when the **vPrefer** policy is set to **Enabled**. This option excludes the native Windows operating system applications like Notepad, Calculator, and so on.
- **Allow network apps**: This option launches the instance of an app that is published on a shared network.

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

> **Limitation:**
>
> This is not supported when using hybrid launches.

Prefer keyword

You can specify that the instance of an app installed on the VDA (referred to as local instance in this document) must be launched in preference to the published application by setting the KEYWORDS:prefer="application" attribute to the application description in **Citrix Studio**.

Before Citrix Workspace app adds **Start** menu shortcuts, it searches for the specified patterns to determine if the application is already installed locally. If it is, Citrix Workspace app 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.

> **Note:**
>
> The keyword prefer is applied when the store is added or the user adds a favorite application. Adding the keyword to an app the user has already added to their favorites has no effect.

> You can specify the prefer keyword multiple times for an application. Only one match is needed to apply the keyword to an application.

The following patterns can be used in any combination:

- prefer="ApplicationName"

  The application name pattern matches any application with the specified application name in the shortcut file name. The application name can be a word or a phrase. Quotation marks are required for phrases. Matching is not allowed on partial words or file paths and is case-insensitive. The application name matching pattern is useful for overrides performed manually by an administrator.

KEYWORDS:PREFER=	SHORTCUT UNDER PROGRAMS	MATCHES?
Word	\Microsoft Office\Microsoft Word 2010	Yes
Microsoft Word	\Microsoft Office\Microsoft Word 2010	Yes
Console	McAfee\VirusScan Console	Yes
Virus	McAfee\VirusScan Console	No
Console	McAfee\VirusScan Console	Yes

- prefer="\\\\Folder1\\Folder2\\...\\ApplicationName"

  The absolute path pattern matches the entire shortcut file path plus the entire application name under the **Start** menu. The Programs folder is a sub folder of the **Start** menu directory, so you must include it in the absolute path to target an application in that folder. Quotation marks are required if the path contains spaces. The matching is case-sensitive. The absolute path matching pattern is useful for overrides implemented programmatically in Citrix Virtual Apps and Desktops™ and Citrix DaaS.

KEYWORDS:PREFER=	SHORTCUT UNDER PROGRAMS	MATCHES?
\Programs\Microsoft Office\Microsoft Word 2010	\Programs\Microsoft Office\Microsoft Word 2010	Yes
\Microsoft Office	\Programs\Microsoft Office\Microsoft Word 2010	No

KEYWORDS:PREFER=	SHORTCUT UNDER PROGRAMS	MATCHES?
\Microsoft Word 2010	\Programs\Microsoft Office\Microsoft Word 2010	No
\Programs\Microsoft Word 2010	\Programs\Microsoft Word 2010	Yes

- prefer="\\Folder1\\Folder2\\...\\ApplicationName"

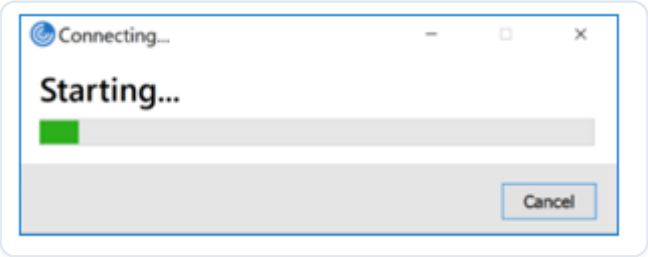
  The relative path pattern matches the relative shortcut file path under the **Start** menu. The relative path provided must contain the application name and can optionally include the folders where the shortcut resides. Matching is successful if the shortcut file path ends with the relative path provided. Quotation marks are required if the path contains spaces. The matching is case-sensitive. The relative path matching pattern is useful for overrides implemented programmatically.

KEYWORDS:PREFER=	SHORTCUT UNDER PROGRAMS	MATCHES?
\Microsoft Office\Microsoft Word 2010	\Microsoft Office\Microsoft Word 2010	Yes
\Microsoft Office	\Microsoft Office\Microsoft Word 2010	No
\Microsoft Word 2010	\Microsoft Office\Microsoft Word 2010	Yes
\Microsoft Word	\Microsoft Word 2010	No

Improved virtual apps and desktops launch experience

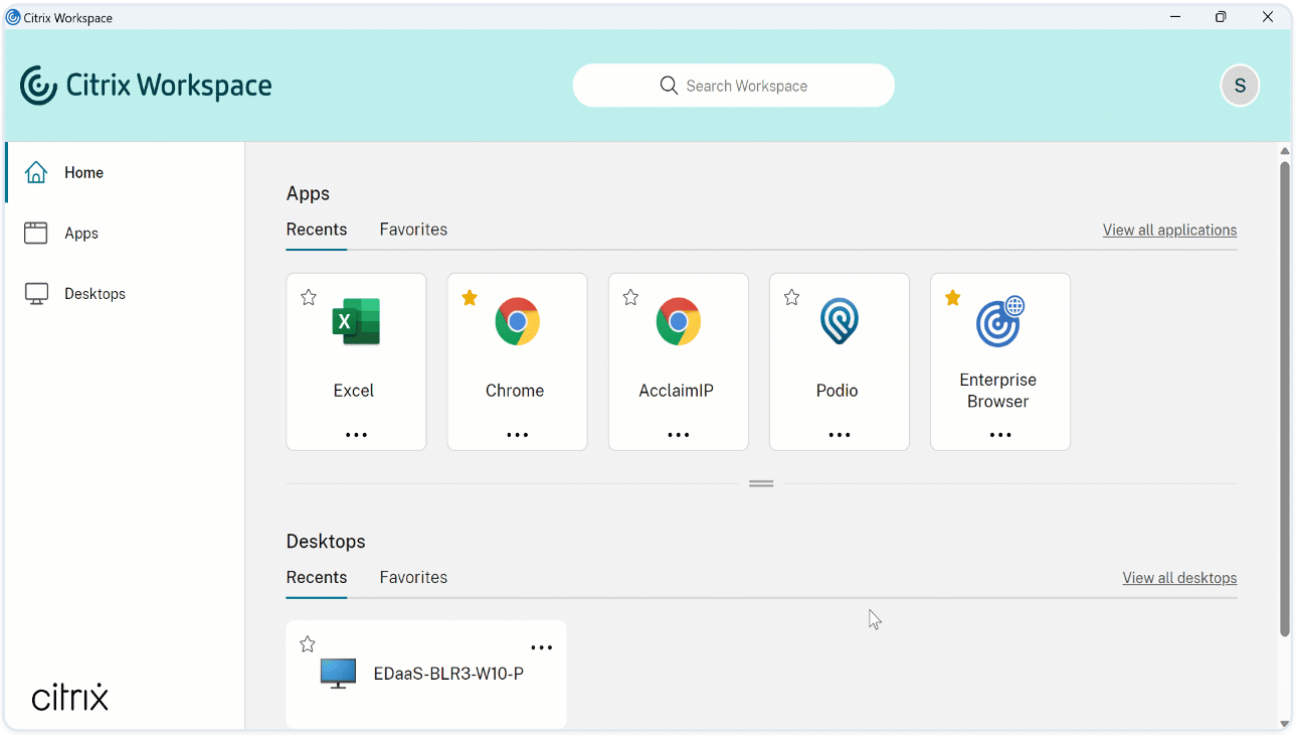
> **Note:**
>
> From Citrix Workspace app version 2305.1 onwards, this feature is generally available for cloud stores and from 2309 for on-premises stores.

> Previously, the launch progress dialog box wasn't intuitive to the users. It made the users assume that the launch process is not responding and they closed the dialog box, as the notification messages were static.



The improved app and desktop launch experience is more informative, modern, and provides a user-friendly experience on Citrix Workspace app for Windows. This new improved launch experience helps to keep the users engaged with timely and relevant information about the launch status. The notification appears in the bottom-right corner of your screen.

Starting with version 2409, Citrix Workspace app for Windows ensures an enhanced desktop launch experience. Now, you experience a seamless, flicker-free transition to your desktop without intermediate screens. The app also eliminates dark screens and flickering during resizing or stretching, providing a stable and modern interface. This feature is enabled by default.



Users can view meaningful notifications about the launch progress, instead of just a spinner. If a launch is in progress and the user attempts to close the browser, a warning message is shown.

Starting with Citrix Workspace app for Windows 2305.1, this feature is enabled by default in cloud stores.

This feature is enabled by default in cloud and in StoreFront (on-premises) session.

App preferences

Advanced Preferences sheet

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

- Hide the Advanced Preferences sheet altogether
- Hide the following, specific settings from the sheet:
    - Data collection
    - Connection Center
    - Configuration checker
    - Keyboard and Language bar
    - High DPI
    - Support information
    - Shortcuts and Reconnect
    - Citrix Casting™

Hiding Advanced Preferences option from the right-click menu

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

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

> **Note:**

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

Hiding specific settings from the Advanced Preferences sheet

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

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

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

OPTIONS	ACTION
Not Configured	Displays the setting
Enabled	Hides the setting
Disabled	Displays the setting

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

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

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

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

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

Hiding Citrix Workspace Updates option from the Advanced Preferences sheet

> **Note:**
>
> The policy path for the Citrix Workspace Updates option is different from 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.

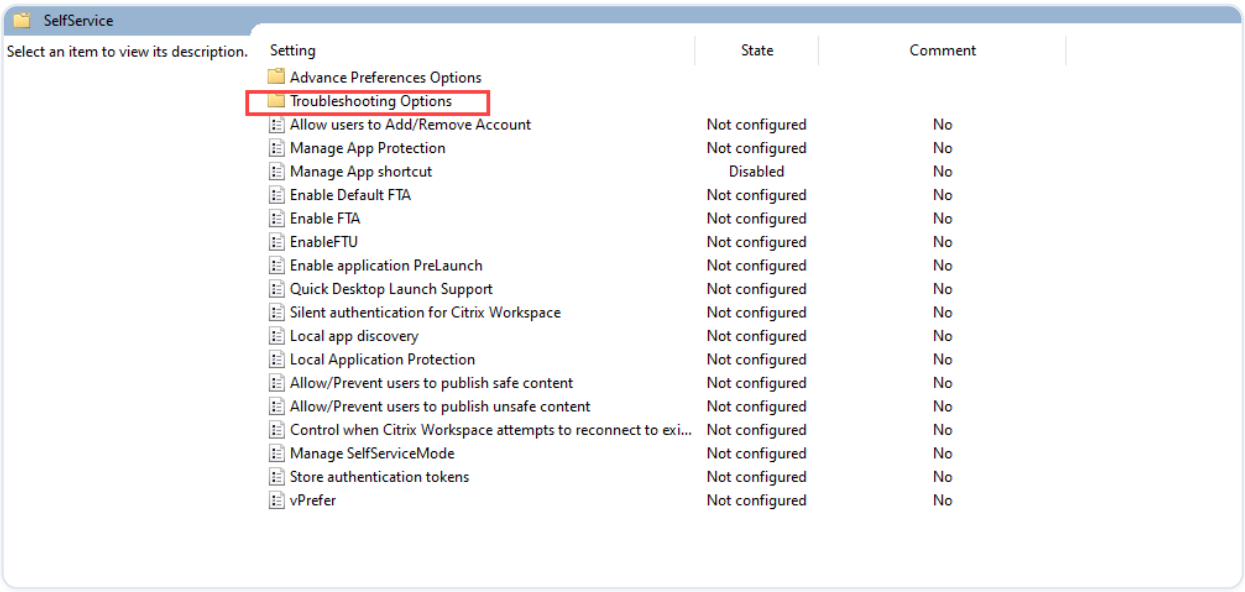
Hide Troubleshooting and Send Feedback options for end-users

Admins can hide the troubleshooting and send feedback options for their end users using the GPO editor. Once this setting is enabled, the **Troubleshooting** and **Send Feedback** options which were previously visible to the end users on the system tray is hidden.

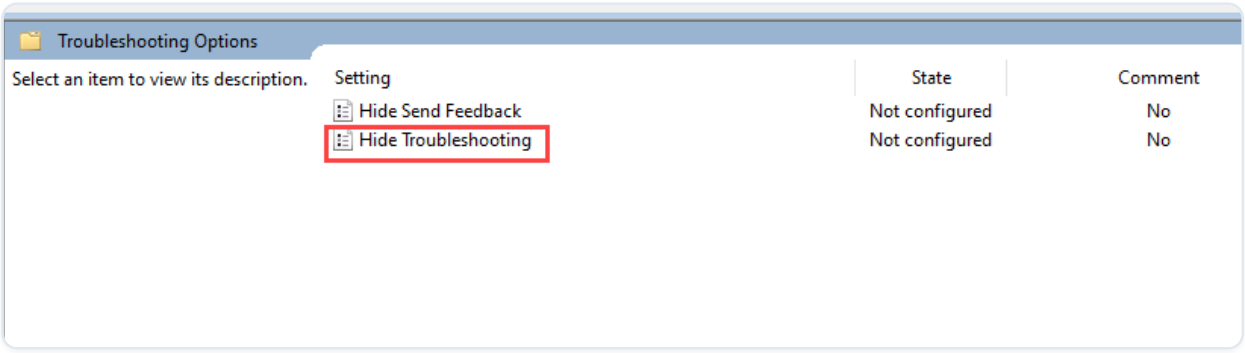
Hide Troubleshooting option

1. On the GPO editor, navigate to **Administrative Templates** > **Citrix Components** > **Citrix Workspace** > **Self Service**.

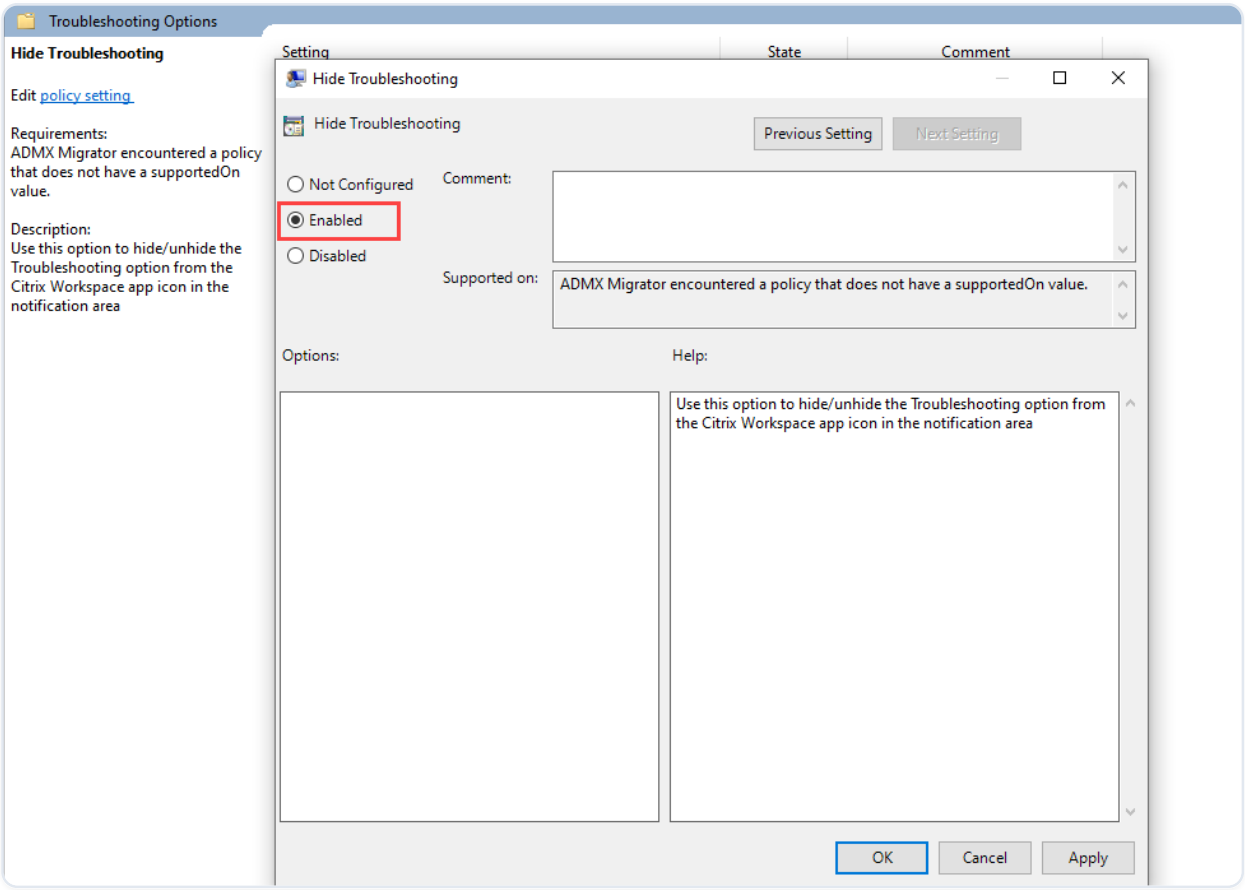
2. Select the **Troubleshooting Options** folder.



3. Select the **Hide Troubleshooting** setting.



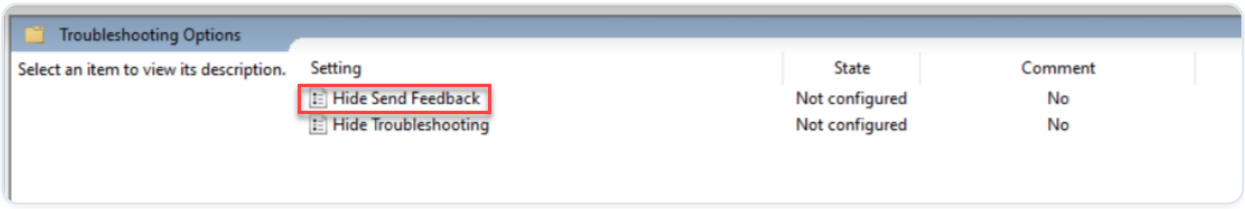
4. On the **Hide Troubleshooting** dialog box, select the **Enabled** checkbox. Selecting this checkbox hides the Troubleshooting option from the end users.



5. Click **OK** to save your settings.

Hide Send Feedback option

1. On the GPO editor, navigate to **Administrative Templates** > **Citrix Components** > **Citrix Workspace** > **Self Service**.
2. Select the **Troubleshooting Options** folder.
3. Select the **Hide Send Feedback** setting.



4. On the **Hide Send Feedback** dialog box, select the **Enabled** checkbox. Selecting this checkbox hides the **Send Feedback** option from the end users.
5. Click **OK** to save your settings.

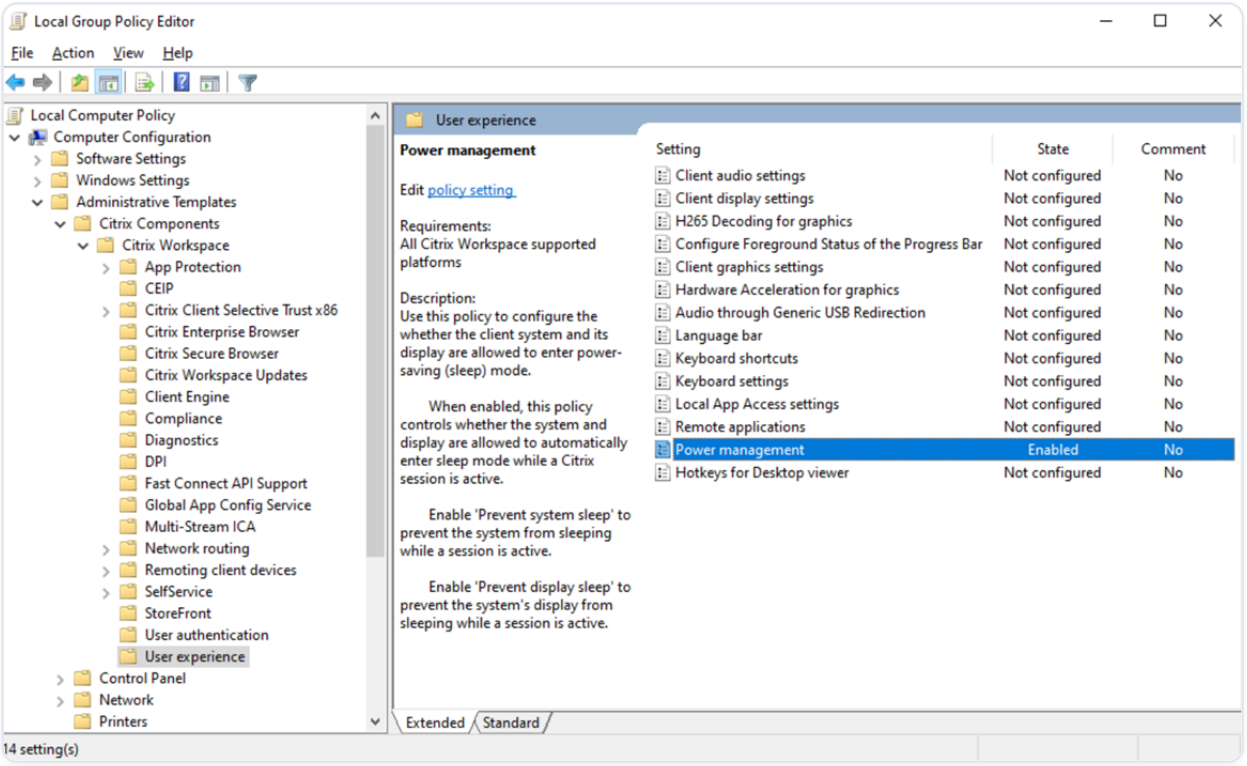
Option to prevent endpoint from going to sleep when a session is active

When a user with an active session stays away from the virtual desktop without any mouse or keyboard activity, the endpoint device might go into sleep mode after completing the set time for Windows sleep mode. As a result, the Citrix® session might be disconnected and when the user returns to the session, the user might be unable to reconnect to the existing session.

With this release, a new policy named **Power Management** is introduced to prevent the endpoint device from going to sleep when a session is active.

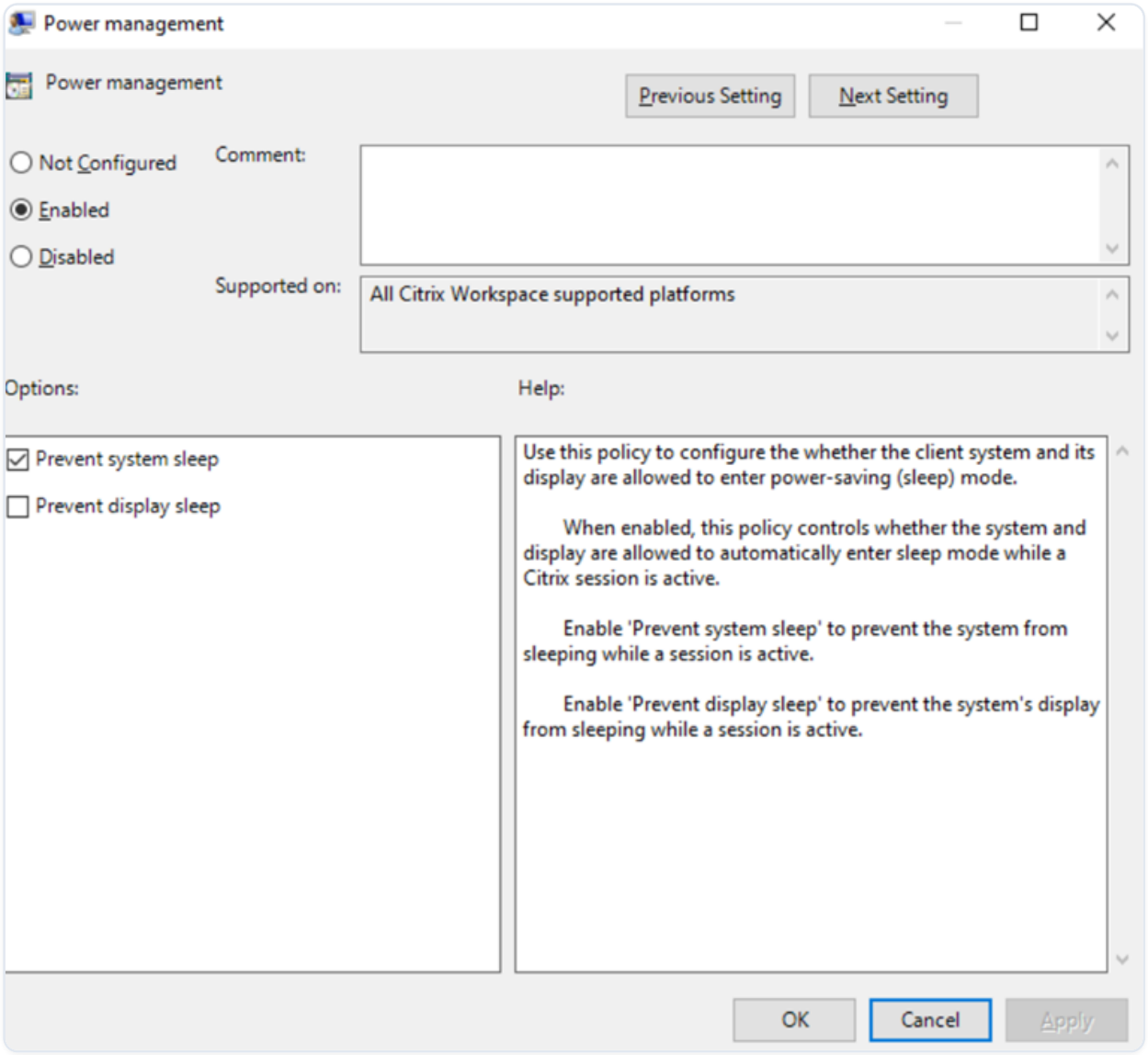
To enable this feature, do the following:

1. Open the Citrix Workspace app Group Policy Object administrative template by running `gpedit.msc`.
2. Under the **Computer Configuration** node, go to **Administrative Templates** > **Citrix Workspace** > **User Experience**.



power-management

3. Select **Power Management**. The **Power Management** screen appears:{}



4. Select **Enabled** and the select the following:

    - **Prevent system sleep** - Select this checkbox to prevent the system from sleeping while a session is active
    - **Prevent display sleep** - Select this checkbox to prevent the system's display from sleeping while a session is active

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

To make the feature available on a per-session basis edit the following registry value:

HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Citrix\ICA Client\Engine\Sleep

To make the feature available on a per-user basis edit the following registry value:

HKEY_CURRENT_USER\Software\Policies\Citrix\ICA Client\Engine\Sleep

Registry values for **Prevent system sleep**:

- Name: AllowSystemSleep
- Type: REG_DWORD
- Value: 0

Registry values for **Prevent display sleep**:

- Name: AllowDisplaySleep
- Type: REG_DWORD
- Value: 0

Auto-sync backend resource changes for Start menu and desktop shortcuts

Starting with 2503 version, the auto-sync backend resource changes feature enhances the user experience by automatically synchronizing backend resource changes for start menu and desktop shortcuts.

Key features include:

- **Updating shortcuts with updated resource path**:

  The shortcut automatically points to the new path when the resource path is updated in the backend, eliminating the need for manual refresh. This feature is enabled by default.

- **Option to show disabled shortcuts**:

  The shortcut remains visible even when a resource is disabled in the backend. Previously, the shortcut was removed when a resource was disabled. This feature is useful for temporary maintenance, allowing users to retain the shortcut. This feature is disabled by default and can be enabled using the **Show Disabled Shortcut** setting in either the Global App Configuration Service (GACS) or the Group Policy Object template.

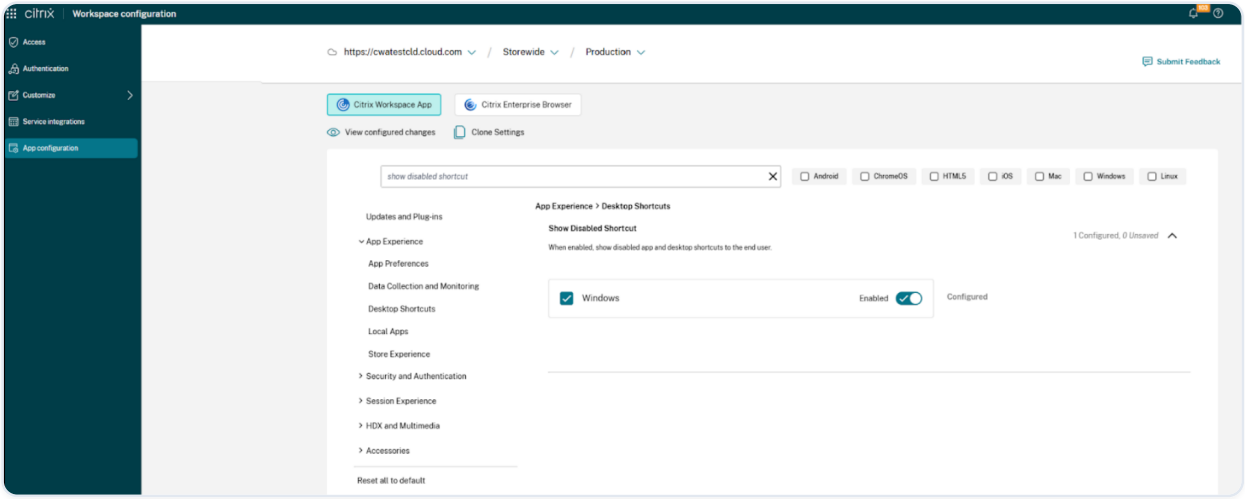
Using GACS

To enable the retention of disabled shortcuts through the GACS Admin UI, do the following:

1. Sign in to citrix.cloud.com with your credentials.

   > **Note:**
   >
   > Refer to the Sign Up for Citrix Cloud article for step-by-step instructions to create a Citrix Cloud account.

2. Upon authentication, click the menu button in the top left corner and select **StoreFront Cloud**. The **StoreFront Cloud** screen appears.
3. Click **App Configuration > Citrix Workspace™ app**.
4. Select the **Windows** checkbox.
5. Update the settings under **App Experience > Show Disabled Shortcuts**.

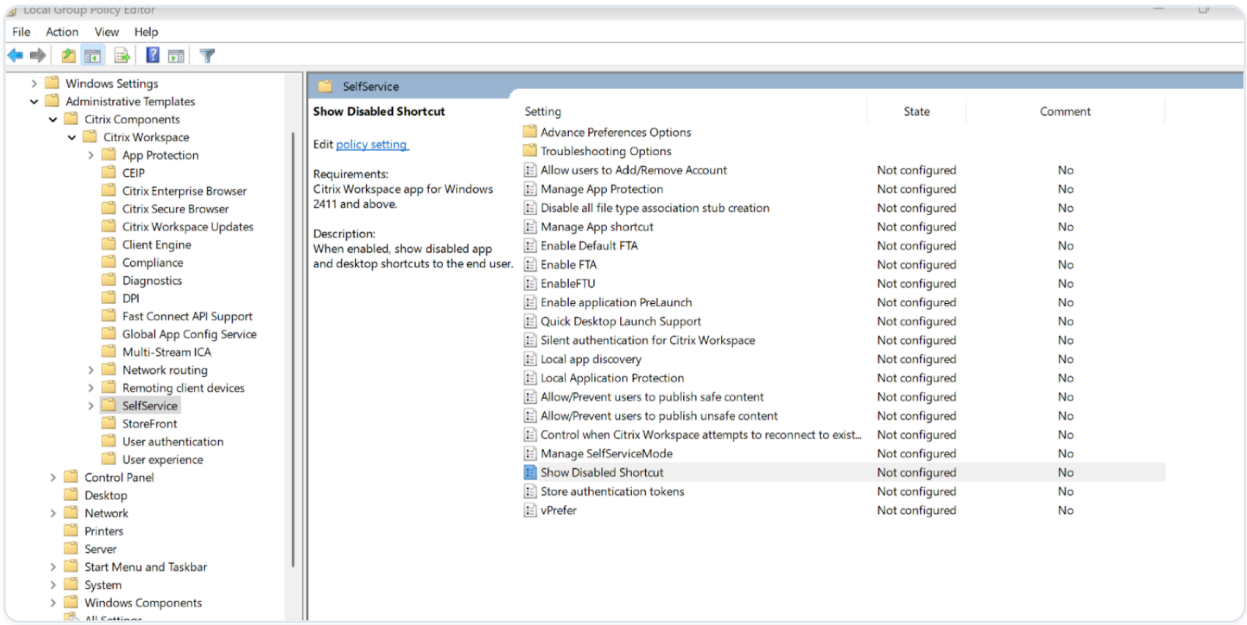


For more information, see the Global App Configuration Service documentation.

Using Group Policy Editor

To customize the options on the **Desktop Viewer** toolbar, do the following:

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 > Self Service** and select **Show Disabled Shortcut**.



3. Select the **Enabled** checkbox.
4. Click **OK**.

Citrix Casting

The Citrix Ready® workspace hub combines digital and physical environments to deliver apps and data within a secure smart space. The complete system connects devices (or things), like mobile apps and sensors, to create an intelligent and responsive environment.

Citrix Ready workspace hub is built on the Raspberry Pi 3 platform. The device running Citrix Workspace app connects to the Citrix Ready workspace hub and casts the apps or desktops on a larger display. Citrix Casting is supported only on Microsoft Windows 10 Version 1607 and later or Windows Server 2016.

Citrix Casting feature allows instant and secure access of any app from a mobile device and display on a large screen.

> **Note:**

> - Citrix Casting for Windows supports Citrix Ready workspace hub Version 2.40.3839 and later. Workspace hub with earlier versions might not get detected or cause a casting error.
> - The Citrix Casting feature is not supported on Citrix Workspace app for Windows (Store).

> **Prerequisites:**

- Bluetooth enabled on the device for hub discovery.
- Both Citrix Ready workspace hub and Citrix Workspace app must be on the same network.
- Port 55555 is allowed between the device running Citrix Workspace app and the Citrix Ready workspace hub.
- For Citrix Casting, port 1494 must not be blocked.
- Port 55556 is the default port for SSL connections between mobile devices and the Citrix Ready workspace hub. You can configure a different SSL port on the Raspberry Pi's settings page. If the SSL port is blocked, users cannot establish SSL connections to the workspace hub.
- Citrix Casting is supported only on Microsoft Windows 10 Version 1607 and later or Windows Server 2016.

- Run `/IncludeCitrixCasting` command during installation to enable Citrix Casting.

Configure Citrix Casting launch

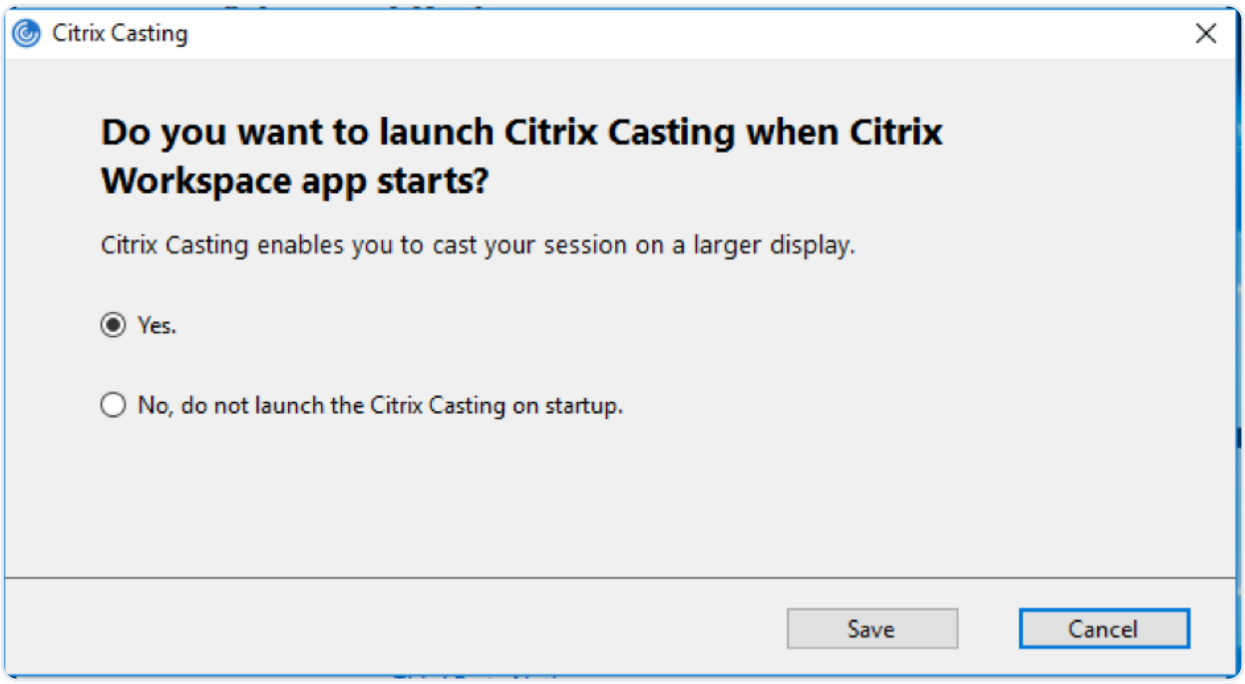
> **Note:**
>
> You can hide all or part of the Advanced Preferences sheet. For more information, see Advanced Preferences sheet.

1. Right-click the Citrix Workspace app icon from the notification area and select **Advanced Preferences**.

   The **Advanced Preferences** dialog appears.

2. Select **Citrix Casting**.

   The **Citrix Casting** dialog appears.



3. Select one of the options:

   - 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:

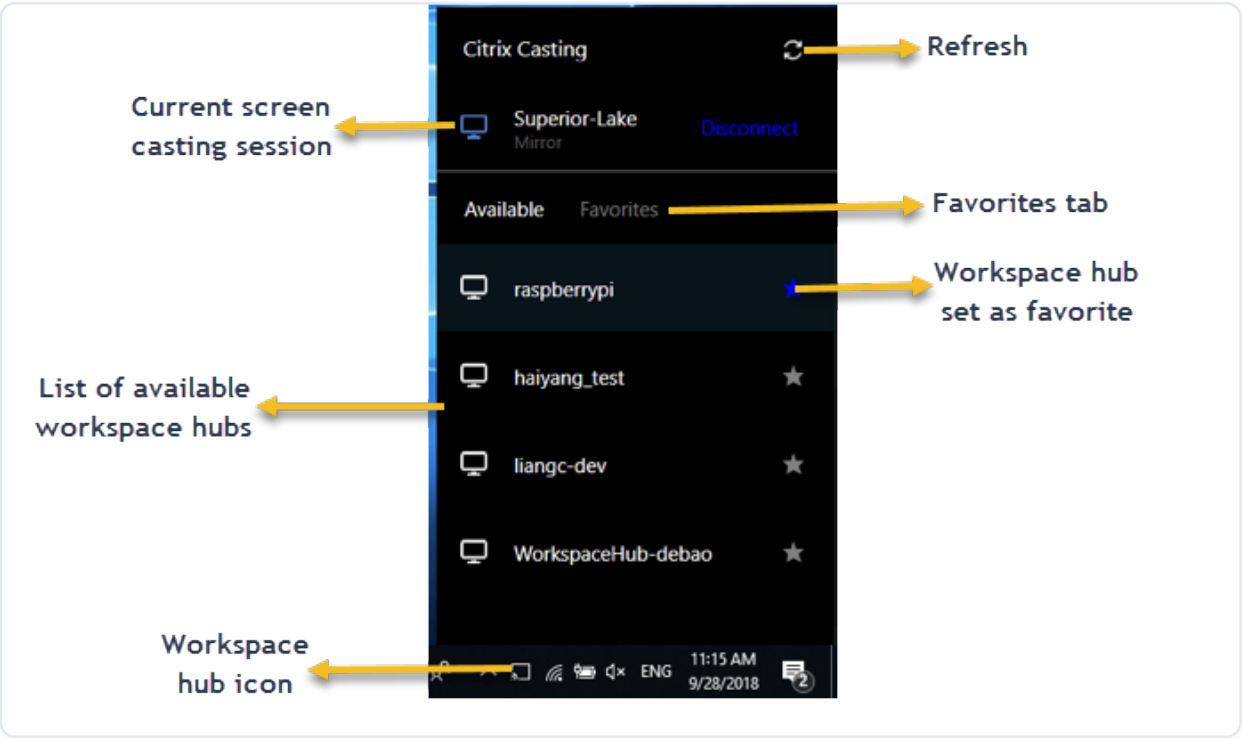
   - **Mirror** to duplicate the primary screen and cast the display to the connected workspace hub device.
   - **Extend** to use the workspace hub device screen as your secondary screen.

> **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 it displays the details of workspace hub device.
5. Click **Refresh** in Citrix Ready workspace hub and try reconnecting to the workspace hub.

Change to Citrix Casting

Previously, Citrix Casting was enabled by default during the Citrix Workspace app installation. Starting from the 2205 release, Citrix Casting is enabled only if you run Citrix Workspace app installer with the `/IncludeCitrixCasting` command during installation. When you update Citrix Workspace app, the Citrix Casting gets updated automatically. For more information on Citrix Casting, see Citrix Casting.

Known issues and limitations

1. Citrix Casting does not work unless the device is connected to the same network as the Citrix Ready workspace hub.
2. If there are network issues, there might be a lag in display on the workspace hub device.
3. When you select **Extend**, the primary screen where Citrix Ready workspace app is launched flashes multiple times.
4. In **Extend** mode, you cannot set the secondary display as the primary display.
5. The screen casting session automatically disconnects when there is any change in the display settings on the device. For example, change in screen resolution, change in screen orientation.
6. During the screen casting session, if the device running Citrix Workspace app locks, sleeps or hibernates, an error appears at login.
7. Multiple screen casting sessions are not supported.
8. The maximum screen resolution supported by Citrix Casting is 1920 x 1440.
9. Citrix Casting supports Citrix Ready workspace hub Version 2.40.3839 and later. Workspace hub with earlier versions might not get detected or cause a casting error.
10. This feature is not supported on Citrix Workspace app for Windows (Store).
11. On Windows 10, Build 1607, Citrix Casting in **Extend** mode might not be properly positioned.

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

SaaS apps

Secure access to SaaS applications provides a unified user experience that delivers published SaaS applications to the users. SaaS apps are available with single sign-on. Administrators can now protect the organization's network and end-user devices from malware and data leaks. Administrators can achieve this by filtering access to specific websites and website categories.

Citrix Workspace app for Windows support the use of SaaS apps using the Citrix Secure Private Access. The service enables administrators to provide a cohesive experience, integrating single sign-on, and content inspection.

Delivering SaaS apps from the cloud has the following benefits:

- Simple configuration – Easy to operate, update, and consume.
- Single sign-on – Hassle-free log on with single sign-on.

- Standard template for different apps – Template-based configuration of popular apps.

Citrix Workspace app launches the SaaS apps on Citrix Enterprise Browser (formerly Citrix Workspace Browser). For information, see Citrix Enterprise Browser documentation.

Limitations:

- When you launch a published app with the print option enabled and download disabled, and give a print command on a launched app, you can still save the PDF. As a workaround, to strictly disable the download functionality, disable the print option.
- Videos embedded in an app might not work.
- You can't open SaaS apps using Storebrowse commands.

For more information about StoreFront Cloud, see StoreFront Cloud in Citrix Cloud.

Data collection and monitoring

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.

Enhancement to Citrix Analytics Service

With this release, Citrix Workspace app is instrumented to securely transmit the public IP address of the most recent network hop to Citrix Analytics Service. This data is collected per session launch. It helps the Citrix Analytics Service to analyze whether poor performance issues are tied to specific geographic areas.

By default, the IP address logs are sent to the Citrix Analytics Service. However, you can disable this option on the Citrix Workspace app using the Registry editor.

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

On 32-bit systems:

- Location: HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\Dazzle
- Name: SendPublicIPAddress
- Type: String

- Value: False

64-bit systems:

- Location: HKEY_LOCAL_MACHINE\Software\Wow6432Node\Citrix\Dazzle
- Name: SendPublicIPAddress
- Type: String
- Value: false

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

> Citrix Workspace app is instrumented to securely transmit data to Citrix Analytics Service from ICA sessions that you launch from a browser.

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

Customer Experience Improvement Program (CEIP)

What is the Citrix Customer Experience Improvement Program (CEIP) for Citrix Workspace app?

The Citrix Customer Experience Improvement Program (CEIP) collects configuration and usage data from the Citrix Workspace app and automatically sends it to Citrix Analytics. This data enables Citrix to analyze the performance and enhance the quality, functionality, and performance of the Citrix Workspace app, optimize resource allocation for product development, and support service levels through effective staffing and infrastructure investment.

All data is used and analyzed solely in aggregate form, ensuring that no individual user or device is singled out or specifically analyzed. Citrix does not collect any Personally Identifiable Information

(PII) through CEIP, and all data collection is in accordance with relevant industry data privacy and security standards.

License telemetry upload using Citrix Workspace™ app

With the the 2507.1 release, you can upload license telemetry data to Citrix Analytics Service through client connections when the license server cannot reach Citrix Analytics service directly.

When your license server loses connectivity to Citrix Analytics service, the feature automatically routes telemetry data through the Virtual Desktop Agent (VDA) and client connection. This ensures continuous license reporting regardless of Customer Experience Improvement Program (CEIP) settings.

Benefits:

- Maintains uninterrupted license telemetry reporting
- Helps preserve compliance requirements
- Provides consistent usage analytics for your Citrix environment
- Works independently of CEIP configuration

Tools used to gather CEIP Data

Citrix Workspace app for Windows uses Citrix Analytics to collect the CEIP data.

Data collected

The specific CEIP data elements collected by Citrix Analytics are:

Operating system version*	Citrix Workspace app version*	Authentication configuration	Citrix Workspace app language
Session launch method	Connection error	Connection protocol	VDA information
Installer configuration	Installer state	Client keyboard layout	Store configuration
Auto-update preference	Connection Center usage	App Protection configuration	Reason for the offline banner
Device Model or Properties	Citrix Virtual Apps and Desktops	Virtual app/desktop name	Auto-update Status

	Session Launch Status		
Connection Lease Details	StoreFront to cloud store URL migration feature usage	Citrix Enterprise Browser Usage	Auto-update channel
Inactivity Timeout Details	Citrix Enterprise Browser Version		

Note:

You can stop sending CEIP data except for the operating system and Citrix Workspace app versions collected for Citrix Analytics indicated by an * in the preceding table.

Which users is CEIP data collected from?

The Citrix Workspace app collects Customer Experience Improvement Program (CEIP) data from its users. CEIP data collected via Citrix Analytics is configured to include users from all regions. To ensure that this functionality is in place, update to the most recent version.

Can users and administrators disable CEIP data collection?

CEIP data collection can be fully disabled in all jurisdictions as per the following configuration.

Starting with version 2205, you can stop sending CEIP data (except for two data elements - Operating System and Citrix Workspace app version) by following these steps:

1. Right-click the Citrix Workspace app icon from the notification area.
2. Select **Advanced Preferences**. The **Advanced Preferences** dialog appears.
3. Choose **Data Collection**.
4. When prompted to send usage statistics and data to Citrix, select **No, Thanks** to disable CEIP participation.
5. Click **Save**.

Alternatively, you can disable CEIP via the registry by navigating to the following entry as an administrator and setting the value:

- Path: HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\ICA Client\CEIP

- Key: Enable_CEIP
- Value: False

After selecting **No, Thanks** or setting the `Enable_CEIP` key to *False*, you can also prevent the final two CEIP data elements (Operating System and Citrix Workspace app version) from being sent. To do so, update the following registry entry:

- Path: HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\ICA Client\CEIP
- Key: DisableHeartbeat
- Value: True

Simplified distribution of uberAgent® on endpoints through Citrix Workspace™ app

uberAgent delivers advanced User Experience and Endpoint Security related insights. Starting with 2507.1 release, uberAgent is now packaged with Citrix Workspace app. This integration supports simplified distribution of uberAgent, streamlining deployment and reducing administrative overhead.

Installation options

Command-line Installation:

- Use `/InstallUberAgent` to install or upgrade the uberAgent plugin.
- Use `/InstallUberAgent /SkipUberAgentUpgrade` to install on devices where uberAgent is not already installed, however skip upgrading it if uberAgent is already present on that device. This option is ideal for VDAs or devices where uberAgent deployment is managed separately from Citrix Workspace app.

Security and authentication

This section describes the following:

- Security
- Secure communications
- Authentication
  - Domain pass-through access matrix
  - Domain pass-through to Citrix Workspace using on-premises Citrix Gateway as the identity provider
  - Domain pass-through to Citrix Workspace using Azure Active Directory as the identity provider
  - Domain pass-through to Citrix Workspace using Okta as identity provider

Security

App Protection

App Protection is an add-on feature that provides enhanced security when using Citrix Virtual Apps and Desktops and Citrix DaaS (formerly Citrix Virtual Apps and Desktops service). Use this feature to:

- restrict the ability of clients to compromise with keylogging and screen capturing malware.
- protect exfiltration of confidential information such as user credentials and sensitive information on the screen.
- prevent users and attackers from taking screenshots and from using keyloggers to glean and exploit sensitive information. For more information, see App Protection.

> **Disclaimer**

> App Protection policies filter the access to required functions of the underlying operating system (specific API calls required to capture screens or keyboard presses). App Protection

policies provide protection even against custom and purpose-built hacker tools. However, as operating systems evolve, new ways of capturing screens and logging keys might emerge. While we continue to identify and address them, we cannot guarantee full protection in specific configurations and deployments.

To configure App Protection on Citrix Workspace app for Windows, see the Citrix Workspace app for Windows section in the Configuration article.

Note:

App Protection is supported only on upgrade from version 1912 onwards.

Seamless integration of deviceTRUST® with Citrix Workspace™ app for Windows

Starting with version 2503, Citrix Workspace app for Windows includes deviceTRUST, enhancing security through continuous device posture checks within the session. deviceTRUST is packaged with Citrix Workspace app for unified deployment, ensuring seamless integration and management. For more information, see deviceTRUST.

Installation

- Citrix Workspace app for Windows always installs or updates deviceTRUST using the packaged version included in the Citrix Workspace app for Windows installer.
- If the deviceTRUST installation fails, you get the **50024** or **50025** error codes, and there is no impact on the installation of Citrix Workspace app for Windows.
- To skip the installation of deviceTRUST, use the `InstallDeviceTrust=N` command from the command line. You can use `InstallDeviceTrust=Y` to install deviceTRUST in case of an upgrade.

Uninstallation

- During uninstallation, Citrix Workspace app removes deviceTRUST only if it installed it.

Auto-update scenarios

- For existing auto-update customers, Citrix Workspace app installs deviceTRUST.

- If the end user has skipped the installation of deviceTRUST in a supported version of Citrix Workspace app, the next cycle of auto-update will also skip the installation of deviceTRUST.

Enhanced security and compatibility with AppLocker

Citrix Workspace app for Windows is compatible with AppLocker, a security posture tool. This feature addresses security concerns and improves the user experience.

ICA® security

When a user launches an app or desktop, StoreFront™ generates ICA information, which contains instructions to the client on how to connect to the VDA.

In-memory hybrid launches

When the user launches a resource, StoreFront generates an ICA file containing instructions on how to connect to the resource. When launched within Citrix Workspace app for Windows, the ICA file is handled within memory and never saved to disk.

When the user opens their store in a web browser and uses Citrix Workspace app for Windows to connect to the resource, it is known as a hybrid launch. Depending on configuration, there are various ways in which the launch can occur, see StoreFront User access options.

Citrix Workspace app for Windows supports Citrix Workspace launcher and Citrix Workspace web extensions for in-memory ICA launches from the user's browser. It is recommended that you disable the user's option to download ICA files. This eliminates surface attacks and any malware that might misuse the ICA file when stored locally. To disable the user's option to download ICA files in StoreFront 2402 and higher, see StoreFront documentation. To disable the user's option to download ICA files in Workspace, see Workspace PowerShell documentation.

Prevent launching of ICA files from disk

Once you have ensured that your own system always uses in-memory launches, Citrix® recommends you to disable launching ICA files from disk. So the users cannot open ICA files they have received from malicious sources by methods such as email. You can disable launching of ICA files from disk, by using any of the following methods:

- Global App Config service
- Group Policy Object (GPO) Administrative template on the client

Global App Config service

You can use the Global App Configuration service from Citrix Workspace app 2106. Under **Security and Authentication** > **Security Preferences**, set the policy **Block Direct ICA File Launches** to enabled.

Group Policy

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

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

ICA file signing

The ICA file signing helps protect you from an unauthorized app or desktop launch. Citrix Workspace app verifies that a trusted source generated the app or desktop launch based on an administrative policy and protects against launches from untrusted servers. You can configure ICA file signing using the GPO administrative template or StoreFront. The ICA file signing feature isn't enabled by default.

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

Configure ICA file signature

> **Note:**
>
> If the CitrixBase.admx\\adml isn't added to the local GPO, the **Enable ICA File Signing** policy might not be present.

1. Open the Citrix Workspace app GPO administrative template by running gpedit.msc
2. Under the **Computer Configuration** node, go to **Administrative Templates** > **Citrix Components**.
3. Select the **Enable ICA File Signing** policy and select one of the options as required:

a. Enabled - Indicates that you can add the signing certificate thumbprint to the allow list of trusted certificate thumbprints.

b. Trust Certificates - Click **Show** to remove the existing signing certificate thumbprint from the allow list. You can copy and paste the signing certificate thumbprints from the signing certificate properties.

c. Security policy - Select one of the following options from the menu.

   i. Only allow signed launches (more secure): Allows only signed app and desktop launches from a trusted server. A security warning appears when there's an invalid signature. The session launch fails because of non-authorization.

   ii. Prompt user on unsigned launches (less secure) - A message prompt appears when an unsigned or invalidly signed session is launched. You can choose to either continue the launch or cancel the launch (default).

4. Click **Apply** and then **OK** to save the policy.
5. Restart the Citrix Workspace app session for the changes to take effect.

When selecting a digital signature certificate, we recommend you choose from the following priority list:

1. Buy a code-signing certificate or SSL signing certificate from a public Certificate Authority (CA).
2. If your enterprise has a private CA, create a code-signing certificate or SSL signing certificate using the private CA.
3. Use an existing SSL certificate.
4. Create a root CA certificate and distribute it to user devices using GPO or manual installation.

Inactivity timeouts

Timeout for Workspace sessions

Admins can configure the inactivity timeout value to specify the amount of idle time allowed before the users automatically sign out of the Citrix Workspace session. You're automatically signed out of Workspace if the mouse, keyboard, or touch is idle for the specified interval of time. The inactivity timeout doesn't affect the active virtual apps and desktops sessions or Citrix StoreFront stores.

To configure inactivity timeout, see the Workspace documentation.

The end-user experience is as follows:

- A notification appears in your session window three minutes before you're signed out, with an option to stay signed in or sign out.
- The notification appears only if the configured inactivity timeout value is greater than or equal to five minutes.
- Users can click **Stay signed in** to dismiss the notification and continue using the app, in which case the inactivity timer is reset to its configured value. You can also click **Sign out** to end the session for the current store.

Timeout for StoreFront sessions

When connected to a StoreFront store, Citrix Workspace app does not apply an inactivity timeout. If you are using a Citrix Gateway, you can configure the gateway's session timeout. For more information, see the StoreFront documentation.

Secure communications

To secure the communication between Citrix Virtual Apps and Desktops server and Citrix Workspace app, you can integrate your Citrix Workspace app connections using a range of secure technologies such as the following:

- Citrix Gateway: For information, see the topics in this section and the Citrix Gateway, and StoreFront documentation.
- A firewall: Network firewalls can allow or block packets based on the destination address and port.
- Transport Layer Security (TLS) versions 1.2 and 1.3 are supported.
- Trusted server to establish trust relations in Citrix Workspace app connections.
- ICA® file signing
- Local Security Authority (LSA) protection
- Proxy server for Citrix Virtual Apps deployments only: A SOCKS proxy server or secure proxy server. Proxy servers help to limit access to and from the network. They also handle the connections between Citrix Workspace app and the server. Citrix Workspace app supports SOCKS and secure proxy protocols.
- Outbound proxy

Citrix Gateway

Citrix Gateway (formerly Access Gateway) secures connections to StoreFront stores. Also, lets administrators control user access to desktops and applications in a detailed way.

To connect to desktops and applications through Citrix Gateway:

1. Specify the Citrix Gateway URL that your administrator provides using one of the following ways:
    - The first time you use the self-service user interface, you are prompted to enter the URL in the **Add Account** dialog box.
    - When you later use the self-service user interface, enter the URL by clicking **Preferences** > **Accounts** > **Add**.
    - If you're establishing a connection with the storebrowse command, enter the URL at the command line

The URL specifies the gateway and, optionally, a specific store:

- To connect to the first store that Citrix Workspace app finds, use a URL in the following format:
    - https://gateway.company.com
- To connect to a specific store, use a URL of the form, for example: https://gateway.company.com?\<storename>. This dynamic URL is in a non-standard form; do not include "=" (the "equals" sign character) in the URL. If you're establishing a connection to a specific store with storebrowse, you might need quotation marks around the URL in the storebrowse command.

1. When prompted, connect to the store (through the gateway) using your user name, password, and security token. For more information about this step, see the Citrix Gateway documentation.

When authentication is complete, your desktops and applications are displayed.

Connecting through firewall

Network firewalls can allow or block packets based on the destination address and port. If you're using a firewall, Citrix Workspace app for Windows can communicate through the firewall with both the Web server and the Citrix server.

Common Citrix Communication Ports

SOURCE	TYPE	PORT	DETAILS
Citrix Workspace app	TCP	80/443	Communication with StoreFront
ICA or HDX	TCP/UDP	1494	Access to applications and virtual desktops
ICA or HDX with Session Reliability	TCP/UDP	2598	Access to applications and virtual desktops
ICA or HDX over TLS	TCP/UDP	443	Access to applications and virtual desktops

For more information about the ports, see the Knowledge Center article CTX101810.

Transport Layer Security

Transport Layer Security (TLS) is the replacement for the SSL (Secure Sockets Layer) protocol. The Internet Engineering Taskforce (IETF) renamed it TLS when it took over responsibility for the development of TLS as an open standard.

TLS secures data communications by providing server authentication, encryption of the data stream, and message integrity checks. Some organizations, including U.S. government organizations, require the use of TLS to secure data communications. These organizations might also require the use of validated cryptography, such as Federal Information Processing Standard (FIPS) 140. FIPS 140 is a standard for cryptography.

To use TLS encryption as the communication medium, you must configure the user device and the Citrix Workspace app. For information about securing StoreFront communications, see the Secure section in the StoreFront documentation. For information about securing VDA, see Transport Layer Security (TLS) in the Citrix Virtual Apps and Desktops documentation.

You can use the following policies to:

- Enforce the use of TLS: We recommend that you use TLS for connections using untrusted networks, including the Internet.

- Enforce the use of FIPS (Federal Information Processing Standards): Approved cryptography and follow the recommendations in NIST SP 800-52. These options are disabled by default.
- Enforce the use of a specific version of TLS and specific TLS cipher suites: Citrix supports the TLS 1.2 and 1.3 protocol.
- Connect only to specific servers.
- Check for revocation of the server certificate.
- Check for a specific server-certificate issuance policy.
- Select a particular client certificate, if the server is configured to request one.

Citrix Workspace app for Windows supports the following cipher suites for TLS 1.2 and 1.3 protocol:

- TLS_AES_256_GCM_SHA384
- TLS_AES_128_GCM_SHA256
- TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384
- TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384
- TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA

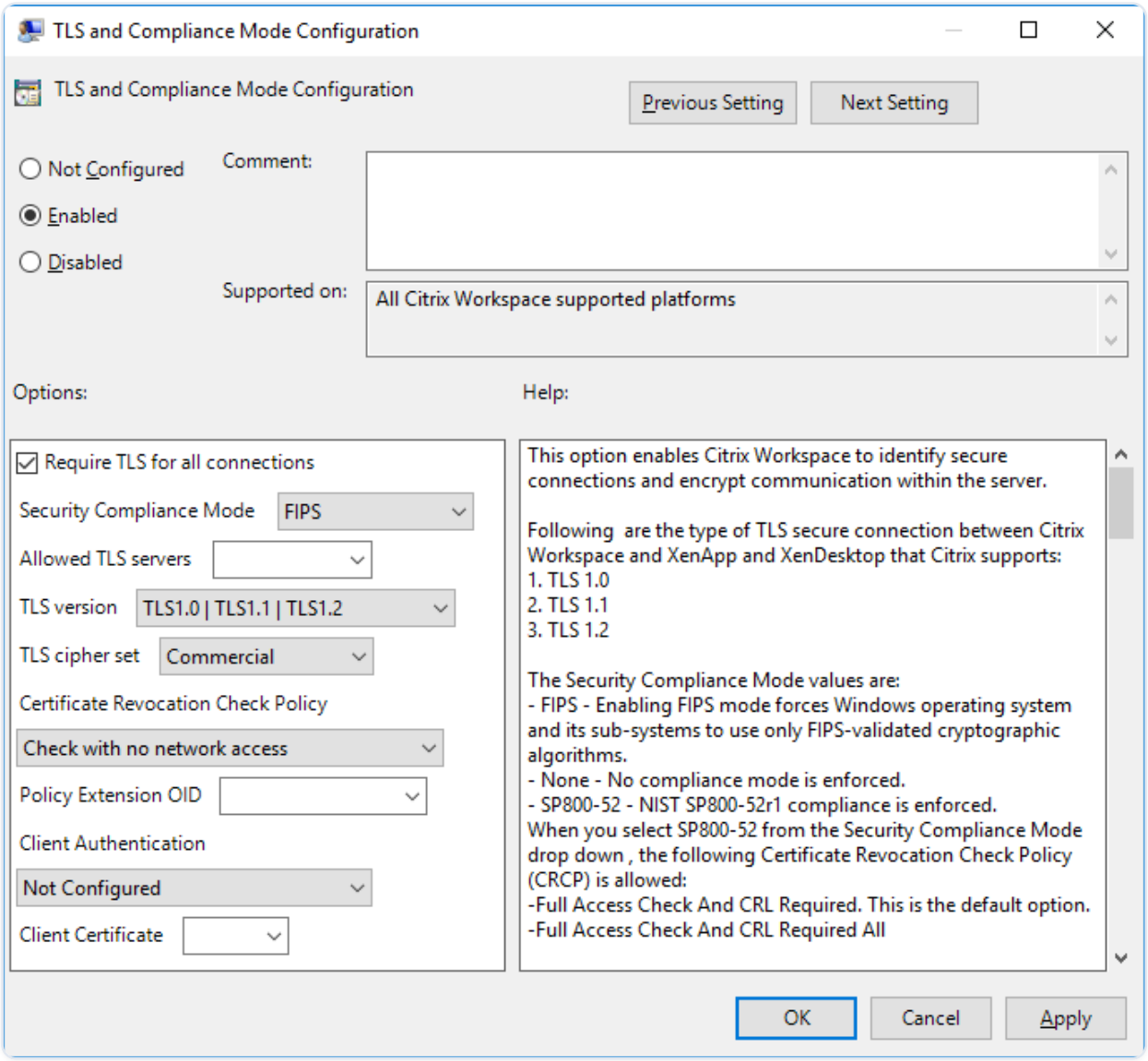
Important:

The following cipher suites are deprecated for enhanced security:

- Cipher suites RC4 and 3DES
- Cipher suites with prefix "TLS_RSA_*"
- TLS_RSA_WITH_AES_256_GCM_SHA384 (0x009d)
- TLS_RSA_WITH_AES_128_GCM_SHA256 (0x009c)
- TLS_RSA_WITH_AES_256_CBC_SHA256 (0x003d)
- TLS_RSA_WITH_AES_256_CBC_SHA (0x0035)
- TLS_RSA_WITH_AES_128_CBC_SHA (0x002f)
- TLS_RSA_WITH_RC4_128_SHA (0x0005)
- TLS_RSA_WITH_3DES_EDE_CBC_SHA (0x000a)

TLS support

1. Open the Citrix Workspace app GPO administrative template by running gpedit.msc.
2. Under the **Computer Configuration** node, go to **Administrative Templates** \> **Citrix Workspace** \> **Network routing**, and select the **TLS and Compliance Mode Configuration** policy.



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

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

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

b. From the **Security Compliance Mode** menu, select the appropriate option:

   i. **None** - No compliance mode is enforced.

   ii. **SP800-52** - Select **SP800-52** for compliance with NIST SP 800-52. Select this option only if the servers or gateway follow NIST SP 800-52 recommendations.

> **Note:**
>
> If you select **SP800-52**, FIPS Approved cryptography is automatically used, even if **Enable FIPS** isn't selected. Also, enable the Windows security option, **System Cryptography: Use FIPS-compliant algorithms for encryption, hashing, and signing**. Otherwise, Citrix Workspace app might fail to connect to the published applications and desktops.
>
> If you select **SP800-52**, set the **Certificate Revocation Check Policy** setting to **Full access check and CRL required**.

When you select **SP800-52**, Citrix Workspace app verifies that the server certificate follows the recommendations in NIST SP 800-52. If the server certificate does not comply, Citrix Workspace app might fail to connect.

   i. **Enable FIPS** - Select this option to enforce the use of FIPS approved cryptography. Also, enable the Windows security option from the operating system group policy, **System Cryptography: Use FIPS-compliant algorithms for encryption, hashing, and signing**. Otherwise, Citrix Workspace app might fail to connect to published applications and desktops.

c. From the **Allowed TLS servers** drop-down menu, select the port number. Use a comma-separated list to ensure that the Citrix Workspace app connects only to a specified server. You can specify wildcards and port numbers. For example, *.citrix.com: 4433 allows connections to any server whose common name ends with .citrix.com on port 4433. The issuer of the certificate asserts the accuracy of the information in a security certificate. If Citrix Workspace does not recognize or trust the issuer, the connection is rejected.

d. From the **TLS version** menu, select one of the following options:

- **TLS 1.0, TLS 1.1, or TLS 1.2** - This is the default setting, which 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 connections use either TLS 1.1 or TLS 1.2.
- **TLS 1.2** - This option is recommended if TLS 1.2 is a business requirement.

a. **TLS cipher set** - To enforce use of a specific TLS cipher set, select Government (GOV), Commercial (COM), or All (ALL).

b. From the **Certificate Revocation Check Policy** menu, select any of the following:

- **Check with No Network Access** - Certificate Revocation list check is done. Only local certificate revocation list stores are used. All distribution points are ignored. A Certificate Revocation List check that verifies the server certificate available from the target SSL Relay/Citrix Secure Web Gateway server isn't mandatory.
- **Full Access Check** - Certificate Revocation List check is done. Local Certificate Revocation List stores and all distribution points are used. If revocation information for a certificate is found, the connection is rejected. Certificate Revocation List check for verifying the server certificate available from the target server isn't critical.
- **Full Access Check and CRL Required** - Certificate Revocation List check is done, except for the root Certificate Authority. Local Certificate Revocation List stores and all distribution points are used. If revocation information for a certificate is found, the connection is rejected. Finding all required Certificate Revocation Lists is critical for verification.
- **Full Access Check and CRL Required All** - Certificate Revocation List check is done, including the root CA. Local Certificate Revocation List stores and all distribution points are used. If revocation information for a certificate is found, the connection is rejected. Finding all required Certificate Revocation Lists is critical for verification.
- **No Check** - No Certificate Revocation List check is done.

a. Using the **Policy Extension OID**, you can limit Citrix Workspace app to connect only to servers with a specific certificate issuance policy. When you select **Policy Extension OID**, Citrix Workspace app accepts only server certificates that contain the Policy Extension OID.

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

- **Disabled** - Client Authentication is disabled.
- **Display certificate selector** - Always prompt the user to select a certificate.
- **Select automatically if possible** - Prompt the user only if there a choice of the certificate to identify.

- **Not configured** - Indicates that client authentication isn't configured.
- **Use specified certificate** - Use the client certificate as set in the Client Certificate option.

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

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

Support for TLS protocol version 1.3

Starting with 2409 version, Citrix Workspace app supports Transport Layer Security protocol (TLS) version 1.3.

> **Note:**
>
> This enhancement requires VDA version 2303 or later.
>
> This feature is enabled by default. To disable it, do the following:

1. Open the Registry Editor using `regedit` on the Run command.
2. Navigate to `HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\Citrix\ICA Client\TLS1.3`.
3. Create a DWORD key by the name `EnableTLS1.3` and set the value of the key to `0`.

Limitations:

- Connections using Access Gateway or NetScaler Gateway Service attempts to use TLS 1.3. However, these connections fallback to TLS 1.2 because Access Gateway and NetScaler Gateway Service doesn’t support TLS 1.3 yet.
- Direct connection to a VDA version that doesn’t support TLS 1.3 fallback to TLS 1.2.

Trusted server

Enforce trusted server connections

Trusted server configuration policy identifies and enforces trust relations in Citrix Workspace app connections.

Using this policy, administrators can control how the client identifies the published application or desktop it is connecting to. The client determines a trust level, called a trust region with a connection. The trust region then determines how the client is configured for the connection.

Enabling this policy prevents connections to the servers that are not in the trusted regions.

By default, region identification is based on the address of the server the client is connecting to. To be a member of the trusted region, the server must be a member of the Windows **Trusted Sites zone**. You can configure this using the **Windows Internet zone** setting.

Alternatively, for compatibility with non-Windows clients, the server address can be specifically trusted using the **Address** setting in the group policy. The server address must be comma-separated list of servers supporting the use of wildcards, for example, `cps*.citrix.com`.

Prerequisite:

- Enusre that you have installed Citrix Workspace app for Windows version 2409 or later.
- Set the DNS resolution to *True* on DDC when using internal storefront and host FQDN in the **Windows Internet options**. For more information, see the Knowledge Center article CTX135250.

> **Note:**
>
> No changes on DDC are required if the IP address is used in the **Windows Internet security zone options**.

- Copy and paste the latest ICA client policies template as per the following table:

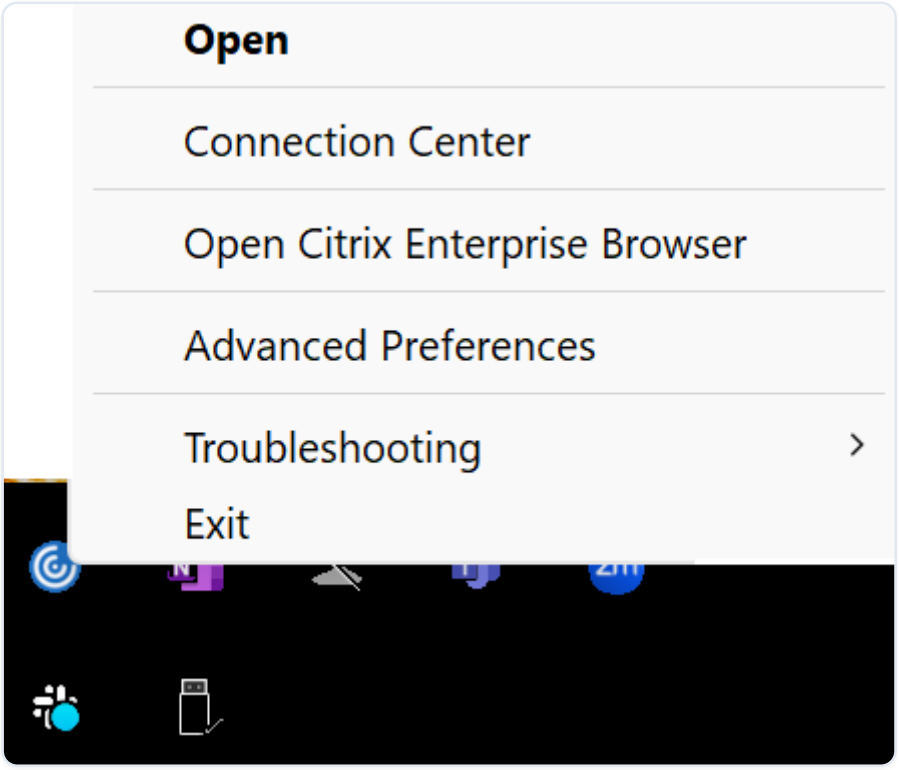
FILE TYPE	COPY FROM	COPY TO
receiver.admx	Installation Directory\ICA Client\Configuration\receiver.admx	%systemroot%\policyDefinitions
CitrixBase.admx	Installation Directory\ICA Client\Configuration\CitrixBase.admx	%systemroot%\policyDefinitions
receiver.adml	Installation Directory\ICA Client\Configuration[MUIculture]receiver.adml	%systemroot%\policyDefinitions[MUIculture]

FILE TYPE	COPY FROM	COPY TO
CitrixBase.adml	Installation Directory\ICA Client\Configuration[MUIculture]\CitrixBase.adml	%systemroot% \policyDefinitions[MUIculture]

Note:

- Ensure that you are using the latest .admx and .adml files included with Citrix Workspace app for Windows version 2409 or later. For more configuration details, see Group policy documentation.

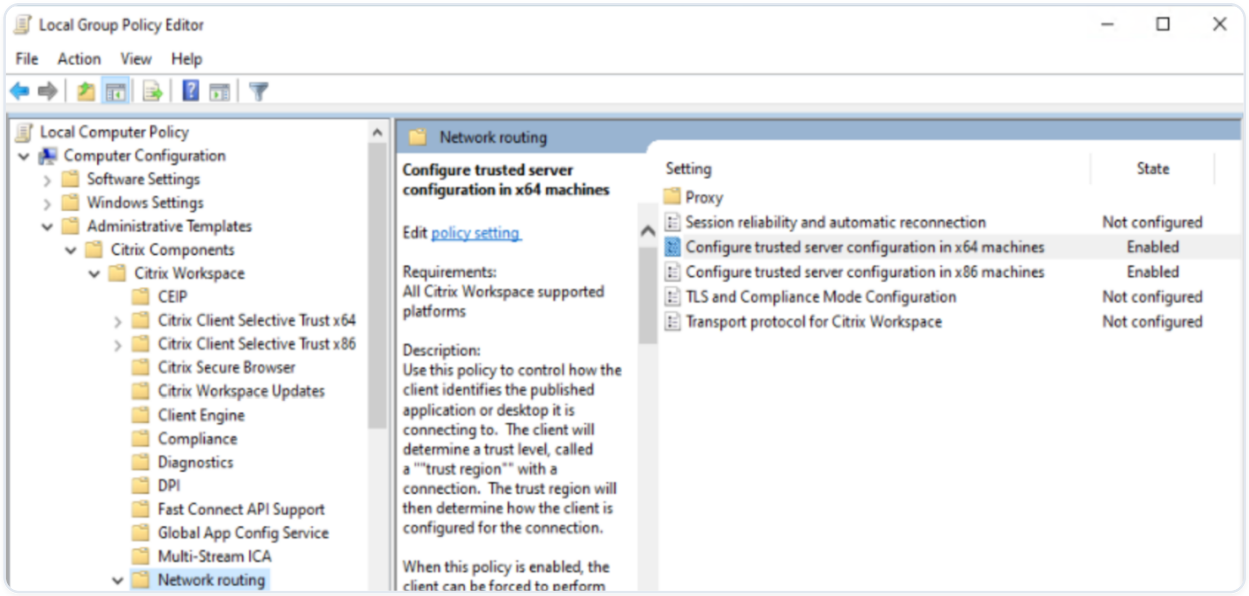
- Close any running Citrix Workspace app instance and exit the same from system tray.



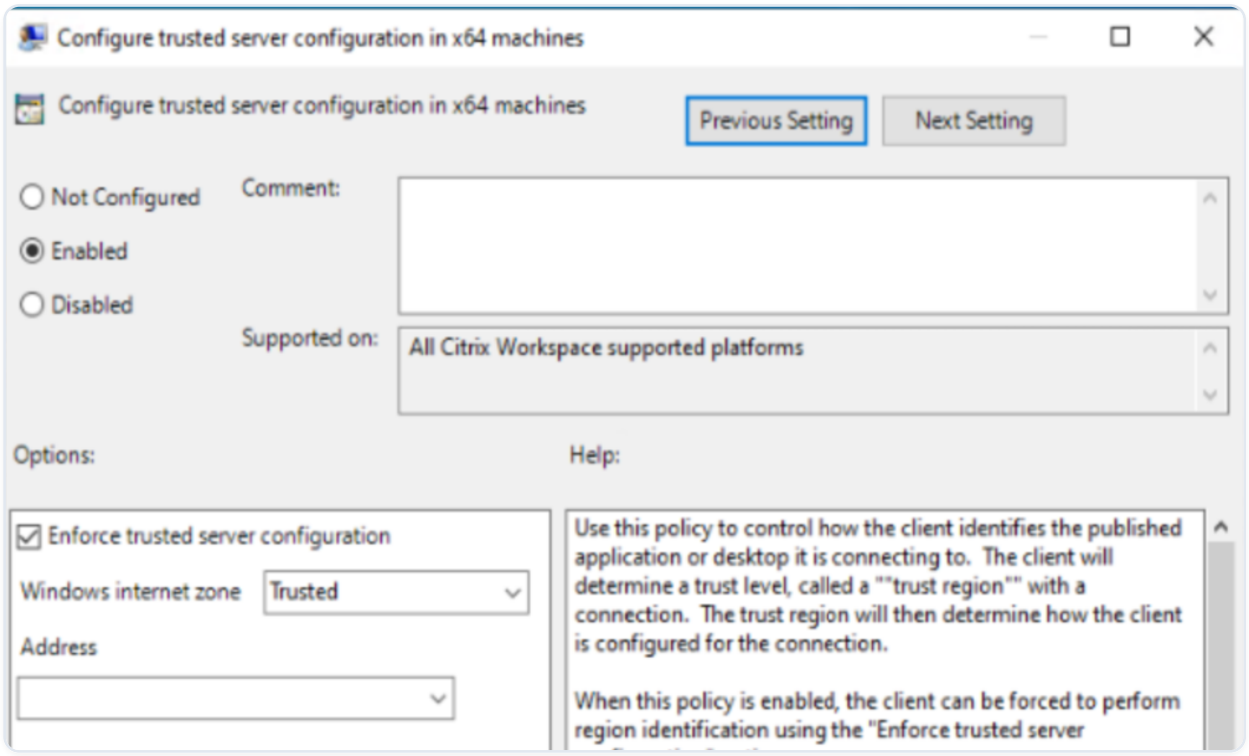
Perform the following steps to enable trusted server configuration using the Group Policy Object administrative template:

1. Open the Citrix Workspace app Group Policy Objective Administrative template by running `gpedit.msc`.
2. Under the **Computer Configuration** node, go to **Administrative Templates** > **Citrix Components** > **Citrix Workspace** > **Network Routing** :

- For x64 deployments, select **Configure trusted server configuration in x64 machines**.
- For x86 deployments, select **Configure trusted server configuration in x86 machines**.



3. Enable the selected policy and select the **Enforce Trusted server configuration** checkbox.
4. From the **Windows internet zone** drop-down menu, select **Trusted**.



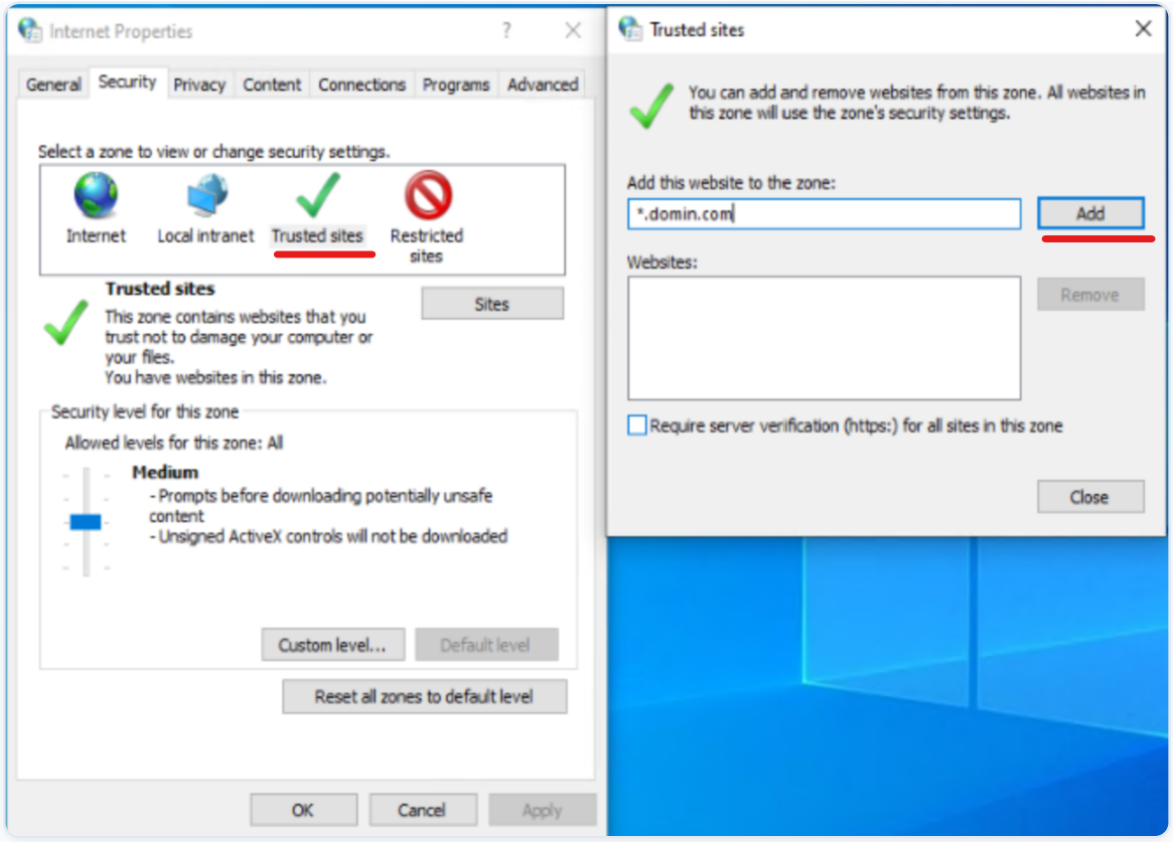
Note:

You can skip selecting options from the **Address** drop-down list.

5. Click **OK** and **Apply**.
6. If the same logged-on user has published Citrix resources, you can proceed with the following or login with a different user.
7. Open **Windows Internet options** and navigate to **Trusted sites** > **Sites** to add a domain address or VDA FQDN into the same.

   Note:

   You can add an invalid domain `*.test.com` or specific invalid or valid VDA FQDN to test the feature.



8. Based on preference, change to **Trusted** or **Local Intranet Sites** based on zone selection in **Windows Internet Zone** within **Configure trusted server configuration policy**.

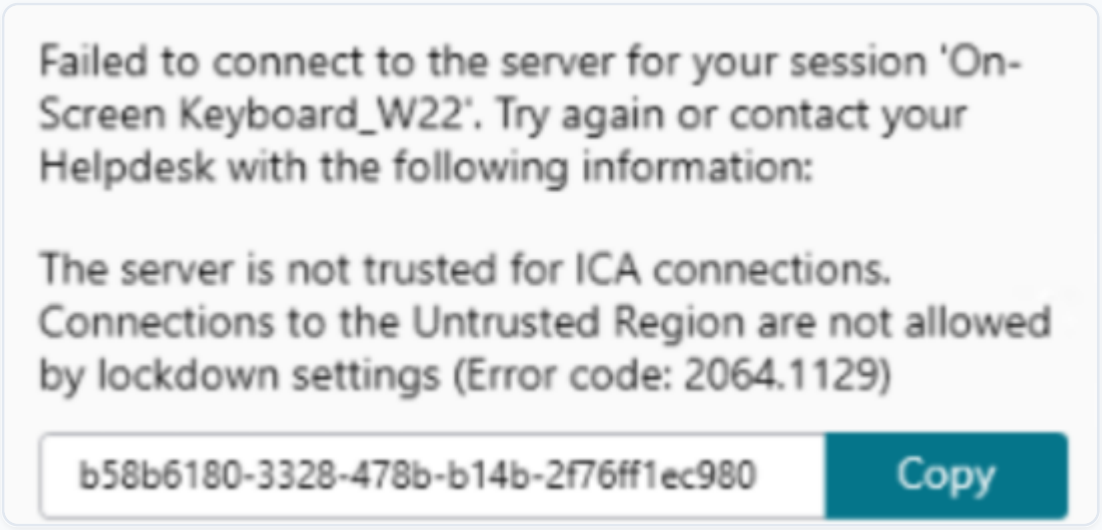
   For more information, see **Modify the Internet Explorer settings** in Authenticate section.
9. Update the Group Policy on the target device where Citrix Workspace app is installed using an admin command prompt or reboot the system.
10. Ensure that the internal StoreFront FQDN is added to the Local Intranet zone or Trusted sites zones based on zone selection in **Windows Internet Zone** within **Configure trusted server**

configuration policy. For information, see **Modify the Internet Explorer settings** in Authenticate section. Also, ensure that in the case of Gateway stores, the Gateway URL must be added to the Trusted sites.

11. Open Citrix Workspace app or published resources and validate the feature.

Note:

If you have not configured the preceding steps, the session launch might fail and you might get the following error message:



As a workaround, you can disable the **Configure trusted server configuration** policy in the GPO.

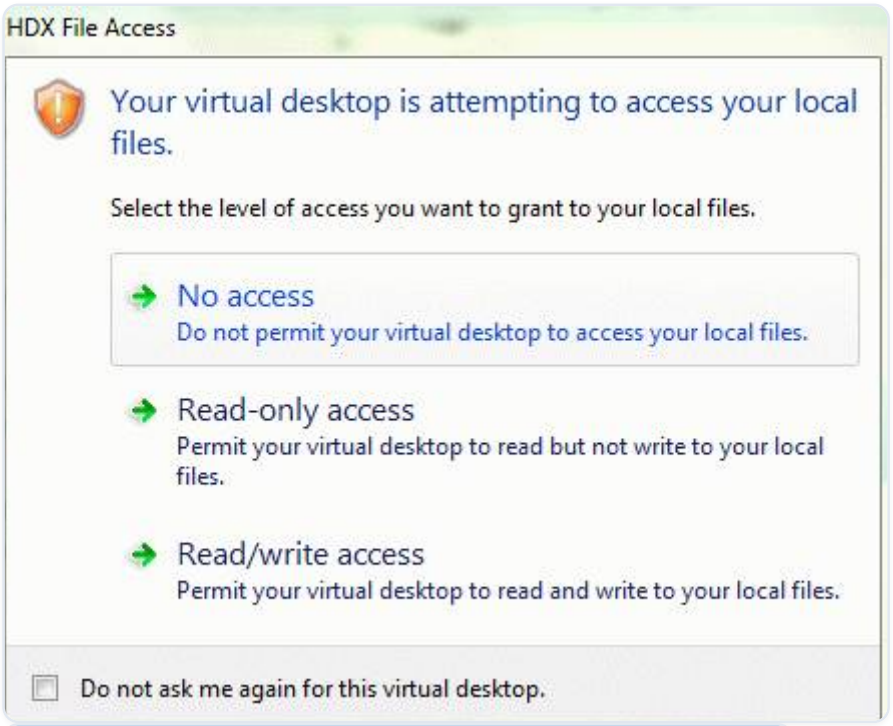
Client selective trust

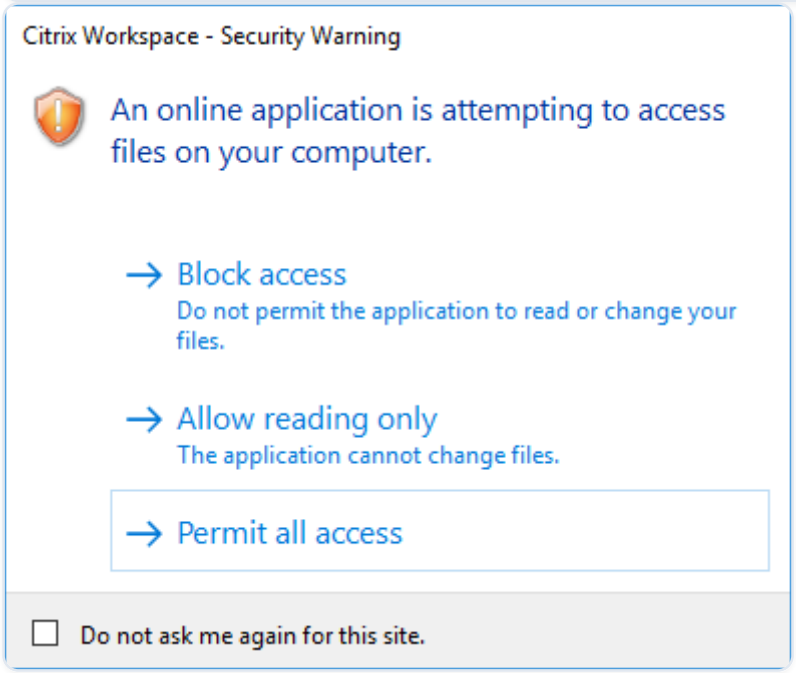
In addition to allowing or preventing connections to the servers, the client also uses the regions to identify file, microphone, or webcam, SSO access.

REGIONS	RESOURCES	ACCESS LEVEL
Internet	File, Microphone, Web	Prompt user for access, SSO is not allowed
Intranet	Microphone, Web	Prompt user for access, SSO is allowed
Restricted Sites	All	No access and connection might be prevented

REGIONS	RESOURCES	ACCESS LEVEL
Trusted	Microphone, Web	Read or write, SSO is allowed

When the user has selected the default value for a region then the following dialog box might appear:







Administrators can modify this default behavior by creating and configuring the **Client Selective Trust** registry keys either using the Group Policy or in the registry. For more information on how to configure Client Selective Trust registry keys, see Knowledge Center article CTX133565.

Client selective trust does not work for direct ICA file download based launches from a browser. For browser-based launches, client selective trust works only when the launch is performed through **WebHelper** or the **Citrix Web Extension**.

Local Security Authority (LSA) protection

Citrix Workspace app supports Windows Local Security Authority (LSA) protection, which maintains information about all aspects of local security on a system. This support provides the LSA level of system protection to hosted desktops.

Connecting through proxy server

Proxy servers are used to limit access to and from your network, and to handle connections between Citrix Workspace app for Windows and servers. Citrix Workspace app supports SOCKS and secure proxy protocols.

When communicating with the server, Citrix Workspace app uses proxy server settings that are configured remotely on the server running workspace for web.

When communicating with the web server, Citrix Workspace app uses the proxy server settings configured through the **Internet** settings of the default web browser on the user device. Configure the **Internet** settings of the default web browser on the user device accordingly.

To enforce proxy settings through the ICA file on StoreFront, see Knowledge Center article CTX136516.

SOCKS5 Proxy Support for EDT

Previously, Citrix Workspace app only supported HTTP proxies operating on TCP. However, SOCKS5 proxy functionality was already fully supported within the Virtual Delivery Agent (VDA). For more information on VDA support, see the Rendezvous V2 documentation.

Starting with 2409 version, Citrix Workspace app now supports SOCKS5 proxies for Enlightened Data Transport (EDT), enhancing compatibility with modern enterprise network configurations.

Key benefits:

- Expanded proxy compatibility: Connect seamlessly through SOCKS5 proxies, widely used by enterprise networking teams for their support of both TCP and UDP traffic.
- Improved EDT performance: Use the full benefits of EDT (UDP-based) for optimized data transfer within Citrix Workspace app sessions.

This feature is disabled by default. To enable this feature, do the following:**

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** > **Proxy** > **Configure client proxy settings** and select the Proxy types.
3. Set the following parameters:
    - **ProxyType**: SocksV5
    - **ProxyHost**: Specify the address of the proxy server.

For more information, see ICA Settings Reference and the Knowledge Center article CTX136516.

Outbound proxy support

SmartControl allows administrators to configure and enforce policies that affect the environment. For instance, you might want to prohibit users from mapping drives to their remote desktops. You can achieve the granularity using the SmartControl feature on the Citrix Gateway.

The scenario changes when the Citrix Workspace app and the Citrix Gateway belong to separate enterprise accounts. In such cases, the client domain can't apply the SmartControl feature because the gateway doesn't exist on the domain. You can then use the Outbound ICA Proxy. The Outbound ICA Proxy feature lets you use the SmartControl feature even when Citrix Workspace app and Citrix Gateway are deployed in different organizations.

Citrix Workspace app supports session launches using the NetScaler LAN proxy. Use the outbound proxy plug-in to configure a single static proxy or select a proxy server at runtime.

You can configure outbound proxies using the following methods:

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

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

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

Outbound proxy support - Configuration

> **Note:**
>
> If both static proxy and dynamic proxies are configured, the dynamic proxy configuration takes precedence.

> **Configuring the outbound proxy using the GPO administrative template:**

1. Open the Citrix Workspace app Group Policy Object administrative template by running gpedit.msc.
2. Under the **Computer Configuration** node, go to **Administrative Templates** > **Citrix Workspace** > **Network routing**.
3. Select one of the following options:
   - For static proxy: Select the **Configure NetScaler® LAN proxy manually** policy. Select **Enabled** and then provide the host name and port number.
   - For dynamic proxy: Select the **Configure NetScaler LAN proxy using DLL** policy. Select **Enabled** and then provide the full path to the DLL file. For example, `C:\Workspace\Proxy\ProxyChooser.dll`.
4. Click **Apply** and **OK**.

Configuring the outbound proxy using the Registry editor:

- **For static proxy:**
  - Launch the Registry editor and navigate to `HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Citrix\ICA Client\Engine\Network Routing\Proxy\NetScaler`.
  - Create DWORD value keys as follows:

    `"StaticProxyEnabled"=dword:00000001`
    `"ProxyHost"="testproxy1.testdomain.com` `"ProxyPort"=dword:000001bb`

- **For dynamic proxy:**
  - Launch the Registry editor and navigate to `HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Citrix\ICA Client\Engine\Network Routing\Proxy\NetScaler LAN Proxy`.
  - Create DWORD value keys as follows: `"DynamicProxyEnabled"=dword:00000001` `"ProxyChooserDLL"="c:\\Workspace\\Proxy\\ProxyChooser.dll"`

Connections and certificates

Connections

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

Certificates

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

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

Private (self-signed) certificates

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

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

Root certificates

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

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

Wildcard certificates

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

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

Intermediate certificates

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

Certificate revocation list

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

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

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

For more information, see the Transport Layer Security section.

Support to mitigate man-in-the-middle attacks

Citrix Workspace app for Windows helps you to reduce the risk of a man-in-the-middle attack using the **Enterprise Certificate Pinning** feature of Microsoft Windows. A man-in-the-middle attack is a type of cyber-attack where the attacker secretly intercepts and relays messages between two parties who believe they are communicating directly with each other.

Previously, when you contact the store server, there was no way to verify whether the response received is from the server you intended to contact or not. Using the **Enterprise Certificate Pinning** feature of Microsoft Windows, you can verify the validity and integrity of the server by pinning its certificate.

Citrix Workspace app for Windows is pre-configured to know what server certificate it must expect for a particular domain or site using the Certificate pinning rules. If the server certificate does not match the pre-configured server certificate, the Citrix Workspace app for Windows prevents the session from taking place.

For information on how to deploy the **Enterprise Certificate Pinning** feature, see the Microsoft documentation.

> **Note:**
>
> You must be aware of the expiry of the certificate and update the group policies and certificate trust lists correctly. Otherwise, you might fail to start the session, even if there is no attack.

Authentication

You can configure various types of authentication for your Citrix Workspace app including domain pass-through (single sign-on or SSON), smart card, and Kerberos pass-through.

Starting with Citrix Workspace™ app for Windows version 2503, the system installs SSON by default in dormant mode. You can enable SSON post-installation using the Group Policy Object (GPO) policy. To enable, navigate to **User Authentication > Local user name and password** and select the **Enable pass-through authentication** checkbox.

> **Note:**
>
> You must reboot the system after updating the GPO policy for the SSON setting to take effect.

Authentication tokens

Authentication tokens are encrypted and stored on the local disk so that you don't need to reenter your credentials when your system or session restarts. Citrix Workspace app provides an option to disable the storing of authentication tokens on the local disk.

For enhanced security, we now provide a Group Policy Object (GPO) policy to configure the authentication token storage.

You can download the Citrix ADMX/ADML templates for Group Policy Editor from the Download page of Citrix.

> **Note:**
>
> This configuration is applicable only in cloud deployments.

> **To disable storing of authentication tokens using the Group Policy Object (GPO) policy:**

1. Open the Citrix Workspace app Group Policy Object administrative template by running `gpedit.msc`.
2. Under the **Computer Configuration** node, go to **Administrative Templates** > **Citrix Components** > **SelfService**.

3. In the **Store authentication tokens** policy, select one of the following:
    - Enabled: Indicates that the authentication tokens are stored on the disk. By default, set to Enabled.
    - Disabled: Indicates that the authentication tokens aren't stored on the disk. Reenter your credentials when your system or session restarts.
4. Click **Apply** and **OK**.

Starting with Version 2106, Citrix Workspace app provides another option to disable the storing of authentication tokens on the local disk. Along with the existing GPO configuration, you can also disable the storing of authentication tokens on the local disk using the Global App Configuration service.

In the Global App Configuration Service, set the `Store Authentication Tokens` attribute to `False`.

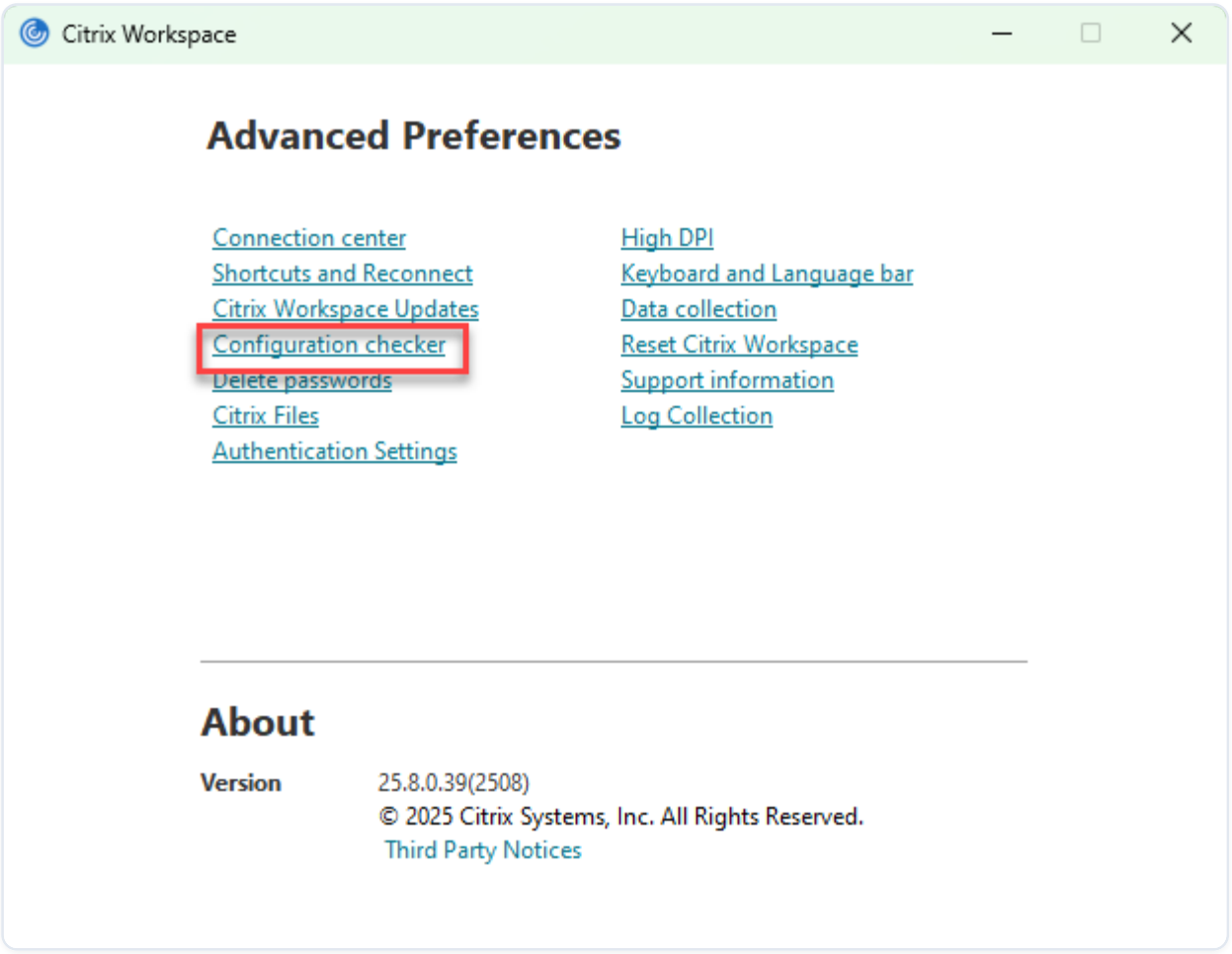
You can configure this setting using the Global App Configuration service in one of the following methods:

- Global App Configuration service User Interface (UI): To configure using UI, see Configure Citrix Workspace app
- API: To configure settings using APIs, see the Citrix Developer documentation.

Configuration Checker

Configuration Checker lets you run a test to check if the single sign-on is configured properly. The test runs on different checkpoints of the single sign-on configuration and displays the configuration results.

1. Right-click the 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 isn't configured properly.
2. **Provider:** Displays the name of the module on which the test is run. In this case, single sign-on.
3. **Suite:** Indicates the category of the test. For example, Installation.
4. **Test:** Indicates the name of the specific test that is run.
5. **Details:** Provides additional information about the test, for both pass and fail.

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

The following tests are done:

1. Installed with single sign-on.
2. Logon credential capture.
3. Network Provider registration: The test result against Network Provider registration displays a green check mark only when "Citrix Single Sign-on" is set to be first in the list of Network Providers. If Citrix Single Sign-on appears anywhere else in the list, the test result against Network Provider registration appears with a blue I and additional information.
4. A single sign-on process is running.
5. Group Policy: By default, this policy is configured on the client.
6. Internet Settings for Security Zones: Make sure that you add the Store/XenApp Service URL to the list of Security Zones in the Internet Options. If the Security Zones are configured via Group policy, any change in the policy requires the **Advanced Preferences** window to be reopened for the changes to take effect and to display the correct status of the test.
7. Authentication method for StoreFront.

> **Note:**
>
> - If you're accessing workspace for web, the test results aren't applicable.
> - If Citrix Workspace app is configured with multiple stores, the authentication method test runs on all the configured stores.
> - You can save the test results as reports. The default report format is .txt.

Hide the Configuration Checker option from the Advanced Preferences window

1. Open the Citrix Workspace app GPO administrative template by running `gpedit.msc`.
2. Go to **Citrix Components** > **Citrix Workspace** > **Self Service** > **DisableConfigChecker**.
3. Click **Enabled** to hide the **Configuration Checker** option from the **Advanced Preferences** window.
4. Click **Apply** and **OK**.
5. Run the `gpupdate /force` command.

Limitation:

Configuration Checker does not include the checkpoint for the configuration of trust requests sent to the XML service on Citrix Virtual Apps and Desktops™ servers.

Beacon test

Citrix Workspace app allows you to do a beacon test using the Beacon checker that is available as part of the **Configuration Checker** utility. The Beacon test helps to confirm if the beacon (ping.citrix.com) is reachable. Starting from Citrix Workspace app for Windows 2405 version onwards, beacon test works for all the beacons configured in the store added in Citrix Workspace app. This diagnostic test helps to eliminate one of the many possible causes for slow resource enumeration that is the beacon not being available. To run the test, right-click the Citrix Workspace app in the notification area and select **Advanced Preferences** > **Configuration Checker**. Select the **Beacon checker** option from the list of Tests and click **Run**.

The test results can be any of the following:

- Reachable – Citrix Workspace app is successfully able to contact the beacon.
- Not reachable - Citrix Workspace app is unable to contact the beacon.
- Partially reachable - Citrix Workspace app can contact the beacon intermittently.

> **Note:**
>
> - The test results aren't applicable on workspace for web.
> - The test results can be saved as reports. The default format for the report is .txt.

Support for Conditional Access with Azure Active Directory

Conditional Access is a tool used by Azure Active Directory to enforce organizational policies. Workspace administrators can configure and enforce Azure Active Directory conditional access policies for users authenticating to the Citrix Workspace app. The Windows machine running the Citrix Workspace app must have Microsoft Edge WebView2 Runtime version 131 or later installed.

For complete details and instructions about configuring conditional access policies with Azure Active Directory, see Azure AD Conditional Access documentation.

> **Note:**
>
> This feature is supported only on Workspace (Cloud) deployments.

Support for modern authentication methods for StoreFront stores

Starting with Citrix Workspace app 2303 for Windows, you can enable support for modern authentication methods for StoreFront stores using Group Policy Object (GPO) template. With Citrix Workspace app version 2305.1, you can enable this feature using Global App Configuration service.

You can authenticate to Citrix StoreFront stores using any of the following ways:

- Using Windows Hello and FIDO2 security keys. For more information, see Other ways to authenticate.
- Single sign-on to Citrix StoreFront stores from Azure Active Directory (AAD) joined machines with AAD as the identity provider. For more information, see Other ways to authenticate.
- Workspace administrators can configure and enforce Azure Active Directory conditional access policies for users authenticating to Citrix StoreFront stores. For more information, see Support for Conditional access with Azure AD.

To enable this feature, you must use Microsoft Edge WebView2 as the underlying browser for direct StoreFront and gateway authentication.

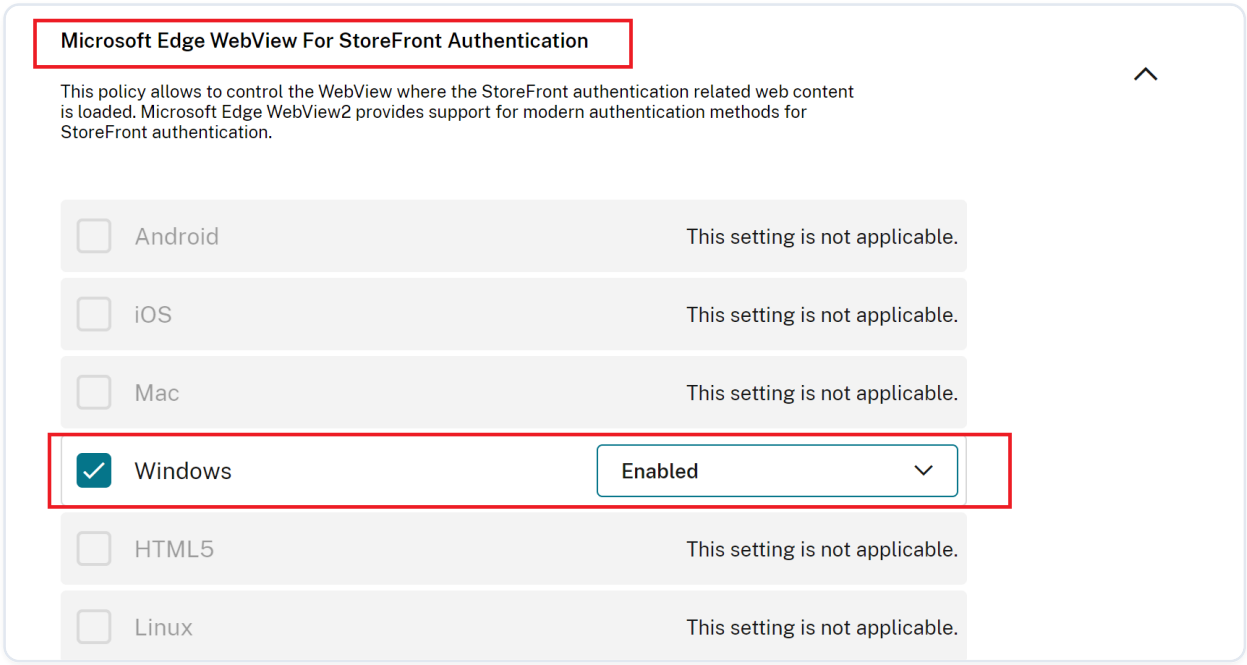
> **Note:**
>
> Ensure that the Microsoft Edge WebView2 Runtime version is 131 or later.

> You can enable modern authentication methods for StoreFront stores using Global App Config service and Group Policy Object (GPO) template.

Using Global App Config service

To enable this feature:

1. From the **Citrix Cloud™** menu, select **StoreFront Cloud** and then select **App Configuration.**
2. Click **Security & Authentication**.
3. Ensure the **Windows** check box is selected.
4. Select **Enabled** next to **Windows** from the **Microsoft Edge WebView for StoreFront™ Authentication** drop-down list.



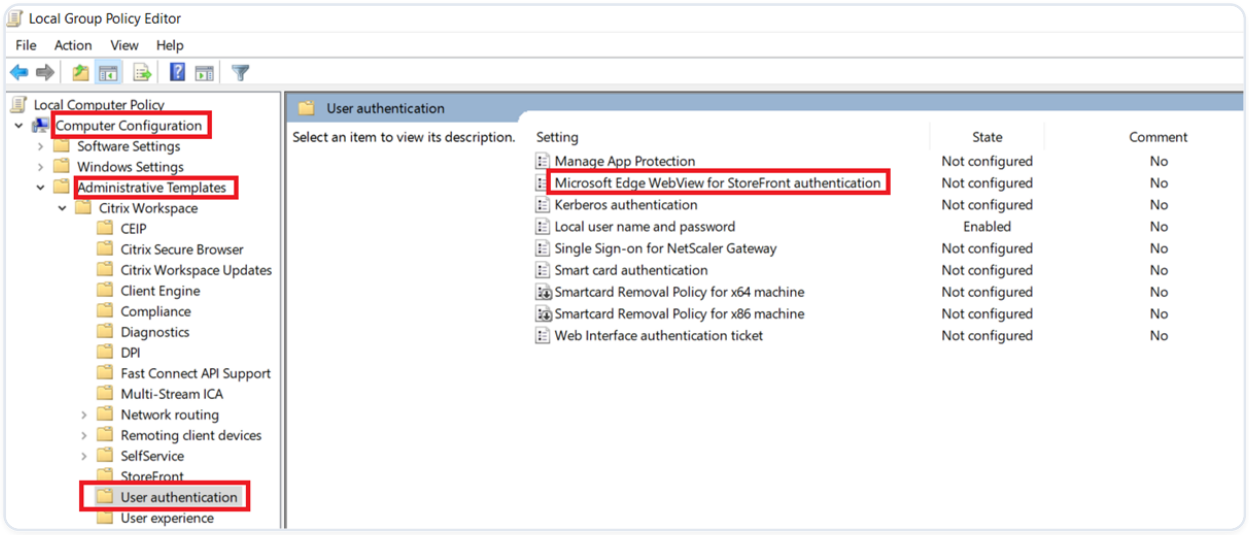
Note:

If you select **Disabled** next to **Windows** from the **Microsoft Edge WebView for StoreFront Authentication** drop-down list, Internet Explorer WebView is used within the Citrix Workspace app. As a result, the modern authentication methods for Citrix StoreFront stores are not supported.

Using GPO

To enable this feature:

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 Authentication**.
3. Click the **Microsoft Edge WebView for StoreFront authentication** policy and set it to **Enabled**.



4. Click **Apply** and then **OK**.

When this policy is disabled, Citrix Workspace app uses Internet Explorer WebView. As a result, the modern authentication methods for Citrix StoreFront stores are not supported.

Single sign-on support for Edge WebView when using Microsoft Entra ID

Previously, when using Entra ID, authentication failed for Citrix Workspace app. Starting with 2409 version, Citrix Workspace app supports single sign-on (SSO) for Edge WebView when using Entra ID for authentication.

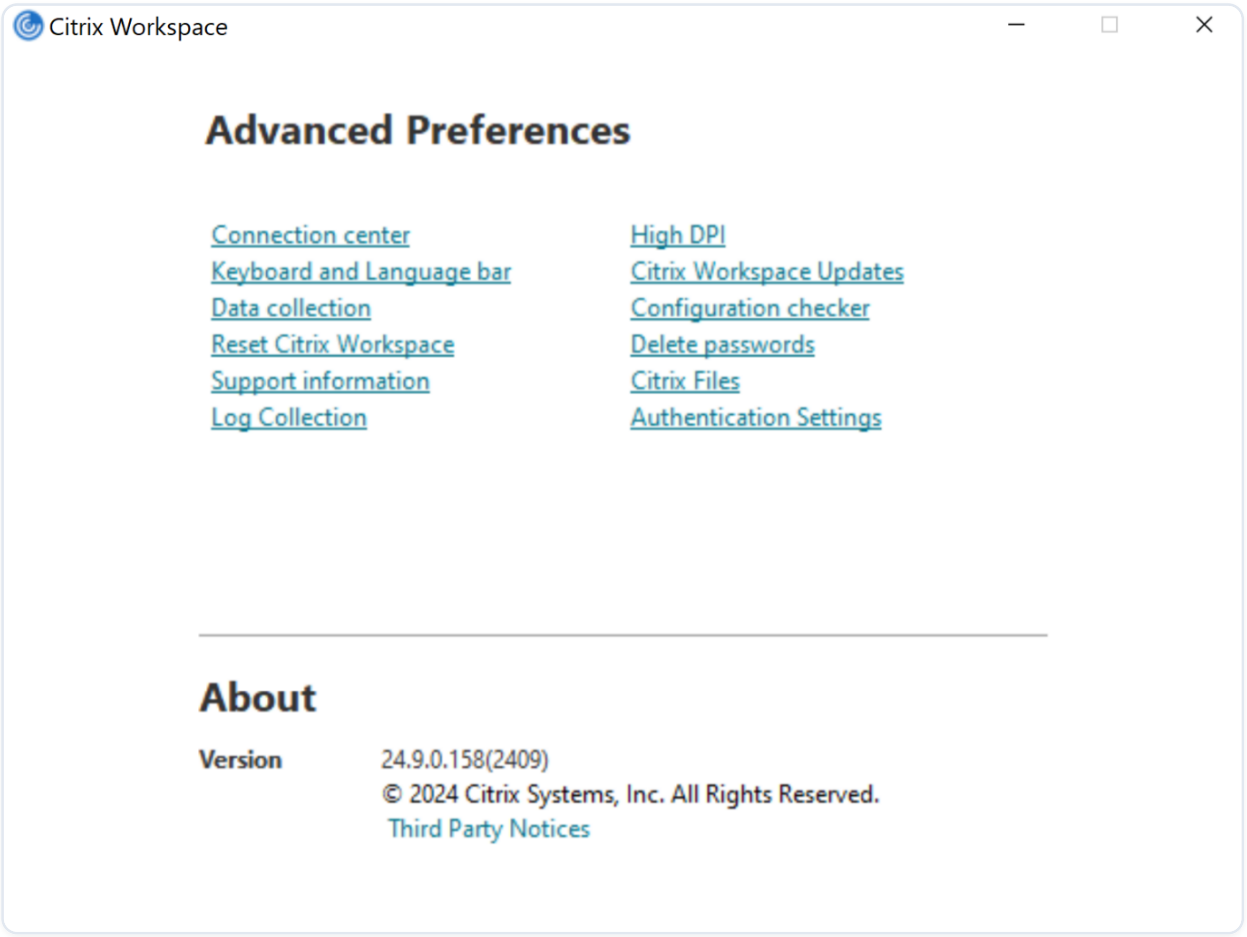
You can enable this feature using the UI or through Group Policy Object (GPO).

Using UI

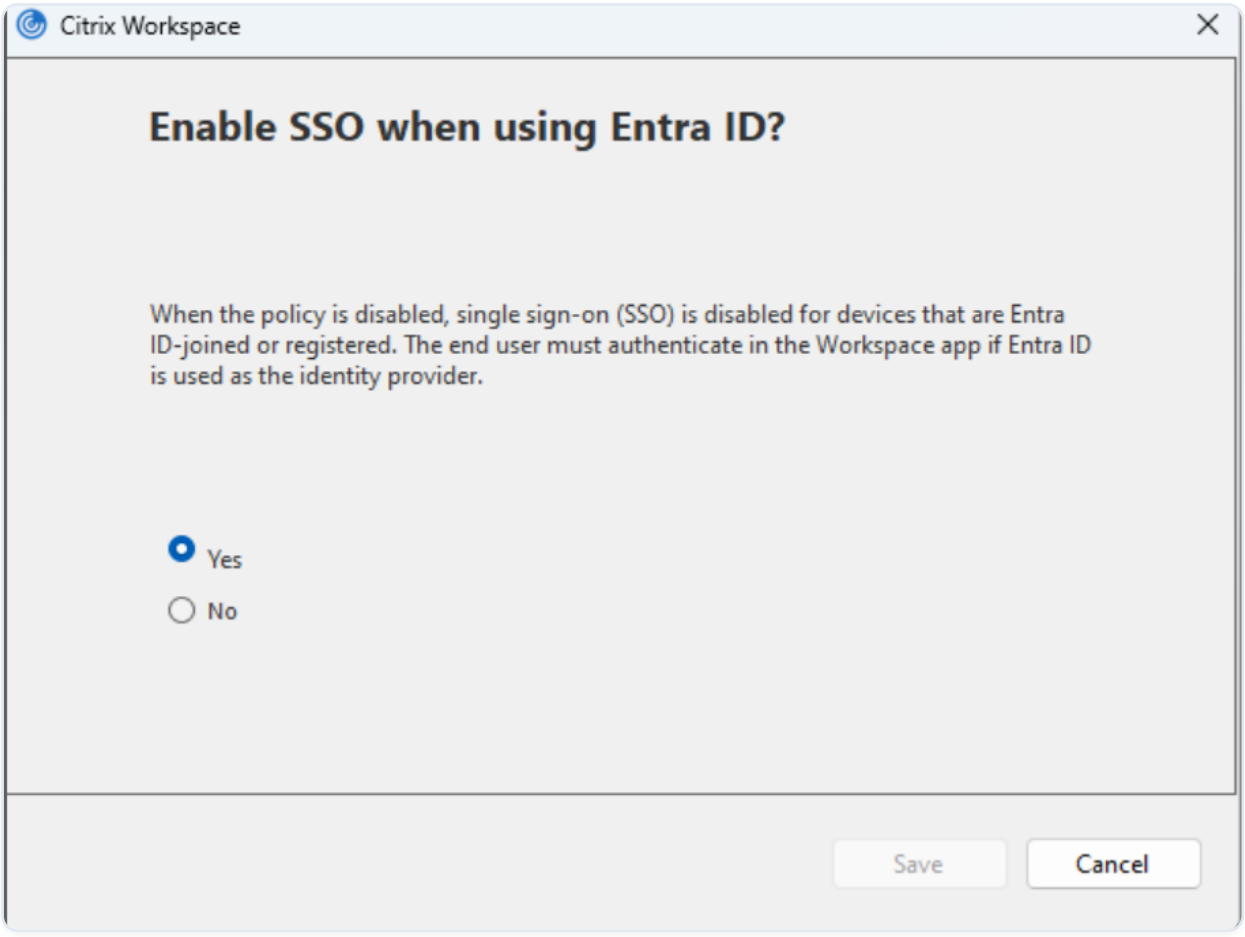
To enable the support for using single sign-on for Edge WebView, a new option called **Authentication Settings** is introduced in the **Advanced Preferences** section of the system tray in the UI.

Perform the following steps to enable the feature from the UI:

1. Click the **Advanced Preferences** section in the system tray. The following screen appears.



2. Click **Authentication Settings**. The following screen appears.



3. Ensure that the option selected is **Yes**, which is the default option. If not, select **Yes**.
4. Click **Save** if you have modified the option.
5. Restart the Citrix Workspace app for the changes to take effect.

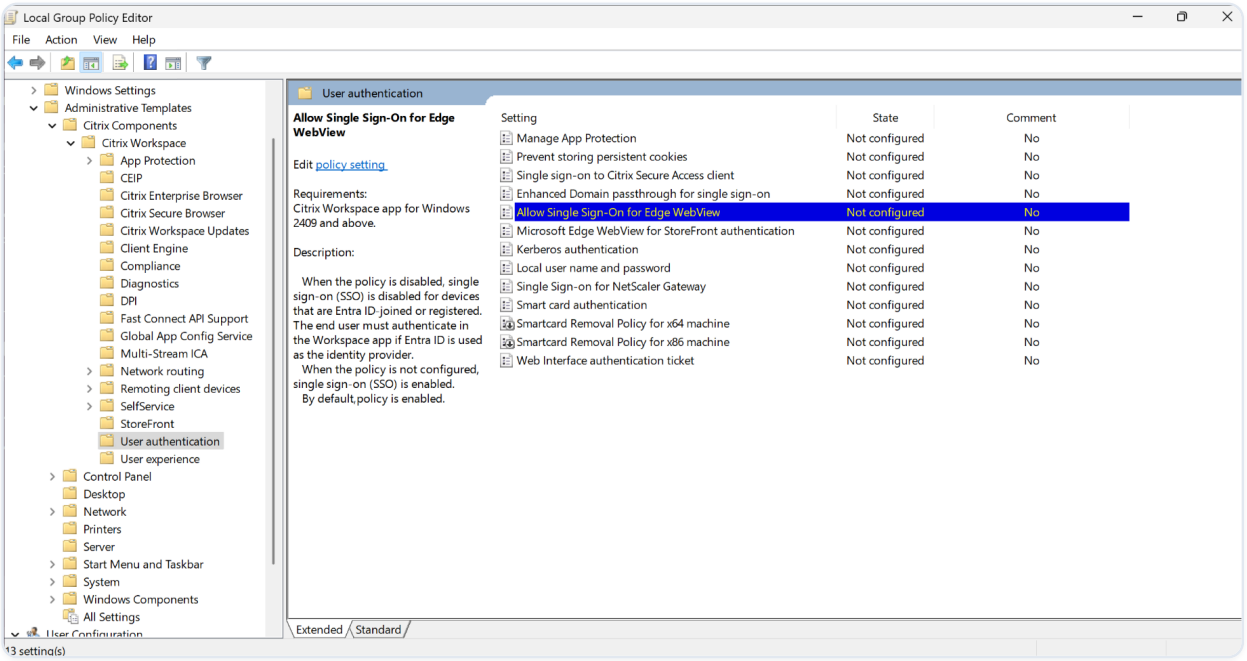
> **Note:**
>
> If you select **No**, the policy is disabled.
>
> When the policy is disabled, single sign-on (SSO) is disabled for devices that are Microsoft Entra ID ID-joined or registered. The end user must authenticate in the Workspace app if Entra ID is used as the identity provider.

Using GPO

You can also enable the support for using single sign-on for Edge WebView using GPO.

Perform the following steps to enable the feature using GPO:

1. Open the Citrix Workspace app Group Policy Object administrative template by running `gpedit.msc` and navigate to the **Computer Configuration** node.



2. Go to **Administrative Templates** > **Citrix Components** > **Citrix Workspace** > **User Authentication**.
3. Select the **Allow Single Sign-On for Edge WebView** policy and set it to **Enabled**.
4. Click **Apply** and **OK**.

> **Note:**

> If you select **Disabled**, the policy is disabled.

> When the policy is disabled, single sign-on (SSO) is disabled for devices that are Microsoft Entra ID ID-joined or registered. The end user must authenticate in the Workspace app if Entra ID is used as the identity provider.

Other ways to authenticate

You can configure the following authentication mechanisms with the Citrix Workspace app. For the following authentication mechanisms to work as expected, the Windows machine running the Citrix Workspace app must have Microsoft Edge WebView2 Runtime version 131 or later installed.

1. Windows Hello based authentication – For instructions about configuring Windows Hello based authentication, see Configure Windows Hello for Business Policy settings - Certificate Trust.

> **Note:**
>
> Windows Hello based authentication with domain pass-through (single-sign-on or SSON) is not supported.

2. FIDO2 Security Keys based authentication – FIDO2 security keys provide a seamless way for enterprise employees to authenticate without entering a user name or password. You can configure FIDO2 Security Keys based authentication to Citrix Workspace. If you would like your users to authenticate to Citrix Workspace with their Azure AD account using a FIDO2 security key, see Enable passwordless security key sign-in.
3. You can also configure Single Sign-On (SSO) to Citrix Workspace app from Microsoft Azure Active Directory (AAD) joined machines with AAD as an identity provider. For more details about configuring Azure Active Directory Domain services, see Configuring Azure Active Directory Domain services. For information about how to connect Azure Active Directory to Citrix Cloud, see Connect Azure Active Directory to Citrix Cloud.

Smart card

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

- **Pass-through authentication (single sign-on)** - Pass-through authentication captures the smart card credentials when users log on to Citrix Workspace app. Citrix Workspace app uses the captured credentials as follows:
  - Users of domain-joined devices who log on to Citrix Workspace app using the smart card can start virtual desktops and applications without needing to reauthenticate.
  - Citrix Workspace app running on non-domain joined devices with the smart card credentials must type their credentials again to start a virtual desktop or application.

  Pass-through authentication requires configuration both on StoreFront and Citrix Workspace app.
- **Bimodal authentication** - Bimodal authentication offers users a choice between using a smart card and typing the user name and password. This feature is effective when you can't use the smart card. For example, the logon certificate has expired. Dedicated stores must be set up per site to allow Bimodal authentication, using the **DisableCtrlAltDel** method set to **False** to allow smart cards. Bimodal authentication requires StoreFront configuration.

Using the Bimodal authentication, the StoreFront administrator can allow both user name and password and smart card authentication to the same store by selecting them in the StoreFront console. See StoreFront documentation.

> **Note:**
>
> Citrix Workspace app for Windows doesn't support umlat character in the **username** and **password** fields.

- **Multiple certificates** - Multiple certificates can be availed for a single smart card and if multiple smart cards are in use. When you insert a smart card in a card reader, the certificates are applicable to all applications running on the user device, including Citrix Workspace app.
- **Client certificate authentication** - Client certificate authentication requires Citrix Gateway and StoreFront configuration.
    - For access to StoreFront through Citrix Gateway, you must reauthenticate after removing the smart card.
    - When the Citrix Gateway SSL configuration is set to **Mandatory client certificate authentication**, operation is more secure. However, mandatory client certificate authentication isn't compatible with bimodal authentication.
- **Double hop sessions** - If a double-hop is required, a connection is established between Citrix Workspace app and the user's virtual desktop.
- **Smart card-enabled applications** - Smart card-enabled applications, such as Microsoft Outlook and Microsoft Office, allow users to digitally sign or encrypt documents available in virtual apps and desktops sessions.

Limitations:

- Certificates must be stored on the smart card and not on the user device.
- Citrix Workspace app does not save the choice of the user certificate, but stores the PIN when configured. The PIN is cached in non-paged memory only during the user session and isn't stored on the disk.
- Citrix Workspace app does not reconnect to a session when a smart card is inserted.
- When configured for smart card authentication, Citrix Workspace app does not support virtual private network (VPN) single-sign on or session pre-launch. To use VPN with smart card authentication, install the Citrix Gateway Plug-in. Log on through a webpage using their smart

cards and PINs to authenticate at each step. Pass-through authentication to StoreFront with the Citrix Gateway Plug-in isn't available for smart card users.

- Citrix Workspace app updater communications with citrix.com and the Merchandising Server aren't compatible with smart card authentication on Citrix Gateway.

> **Warning**
>
> Some configuration requires registry edits. Using the Registry editor incorrectly might cause problems that can require you to reinstall the operating system. Citrix can't guarantee that problems resulting from incorrect use of the Registry Editor can be solved. Make sure you back up the registry before you edit it.

> **To enable single sign-on for smart card authentication:**

To configure Citrix Workspace app for Windows, include the following command-line option during installation:

- `ENABLE_SSON=Yes`

  Single sign-on is another term for pass-through authentication. Enabling this setting prevents Citrix Workspace app from displaying a second prompt for a PIN.

- In the Registry editor, navigate to the following path and set the `SSONCheckEnabled` string to `False` if you have not installed the single sign-on component.

  `HKEY_CURRENT_USER\Software{Wow6432}\Citrix\AuthManager\protocols\integratedwindows\`

  `HKEY_LOCAL_MACHINE\Software{Wow6432}\Citrix\AuthManager\protocols\integratedwindows\`

  The key prevents the Citrix Workspace app authentication manager from checking for the single sign-on component and allows Citrix Workspace app to authenticate to StoreFront.

To enable smart card authentication to StoreFront instead of Kerberos, install Citrix Workspace app for Windows with the following command-line options:

- `/includeSSON` installs single sign-on (pass-through) authentication. Enables credential caching and the use of pass-through domain-based authentication.
- If the user logs on to the endpoint with a different authentication method, for example, user name and password, the command line is:

```
/includeSSON LOGON_CREDENTIAL_CAPTURE_ENABLE=No
```

This type of authentication prevents capturing of the credentials at logon time and allows Citrix Workspace app to store the PIN during Citrix Workspace app login.

1. Open the Citrix Workspace app Group Policy Object administrative template by running gpedit.msc.
2. Go to **Administrative Templates** \> **Citrix Components** \> **Citrix Workspace** \> **User Authentication** \> **Local user name and password**.
3. Select **Enable pass-through authentication**. Depending on the configuration and security settings, select **Allow pass-through authentication for all ICA® option** for pass-through authentication to work.

To configure StoreFront:

- When you configure the authentication service, select the **Smart card** check box.

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

To enable user devices for smart card use:

1. Import the certificate authority root certificate into the device's keystore.
2. Install your vendor's cryptographic middleware.
3. Install and configure Citrix Workspace app.

To change how certificates are selected:

By default, if multiple certificates are valid, Citrix Workspace app prompts the user to choose a certificate from the list. Instead, you can configure Citrix Workspace app to use the default certificate (per the smart card provider) or the certificate with the latest expiry date. If there are no valid logon certificates, the user is notified, and given the option to use an alternate logon method if available.

A valid certificate must have all of these characteristics:

- The current time of the clock on the local computer is within the certificate validity period.
- The **Subject public** key must use the RSA algorithm and have a key length of 1024 bits, 2048 bits, or 4096 bits.
- Key usage must include digital signature.

- Subject Alternative Name must include the User Principal Name (UPN).
- Enhanced key usage must include smart card logon and client authentication, or all key usages.
- One of the Certificate Authorities on the certificate's issuer chain must match one of the allowed Distinguished Names (DN) sent by the server in the TLS handshake.

Change how certificates are selected by using either of the following methods:

- On the Citrix Workspace app command line, specify the option `AM_CERTIFICATESELECTIONMODE={ Prompt | SmartCardDefault | LatestExpiry }`.

  Prompt is the default. For `SmartCardDefault` or `LatestExpiry`, if multiple certificates meet the criteria, Citrix Workspace app prompts the user to choose a certificate.
- Add the following key value to the registry key `HKEY_CURRENT_USER OR HKEY_LOCAL_MACHINE\Software\[Wow6432Node\Citrix\AuthManager`: CertificateSelectionMode={ Prompt | SmartCardDefault | LatestExpiry }.

Values defined in `HKEY_CURRENT_USER` take precedence over values in `HKEY_LOCAL_MACHINE` to best assist the user in selecting a certificate.

To use CSP PIN prompts:

By default, the PIN prompts presented to users are provided by Citrix Workspace app for Windows rather than the smart card Cryptographic Service Provider (CSP). Citrix Workspace app prompts users to enter a PIN when required and then passes the PIN to the smart card CSP. If your site or smart card has more stringent security requirements, such as to disallow caching the PIN per-process or per-session, you can configure Citrix Workspace app to use the CSP components to manage the PIN entry, including the prompt for a PIN.

Change how PIN entry is handled by using either of the following methods:

- On the Citrix Workspace app command line, specify the option `AM_SMARTCARDPINENTRY=CSP`.
- Add the following key value to the registry key `HKEY_LOCAL_MACHINE\Software\[Wow6432Node\Citrix\AuthManager`: SmartCardPINEntry=CSP.

Smart card support and removal changes

A Citrix Virtual Apps session logs off when you remove the smart card. If Citrix Workspace app is configured with smart card as the authentication method, configure the corresponding policy on

Citrix Workspace app for Windows to enforce the Citrix Virtual Apps session for logoff. The user is still logged into the Citrix Workspace app session.

Limitation:

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

Fast smart card

Fast smart card is an improvement over the existing HDX PC/SC-based smart card redirection. It improves performance when smart cards are used in high-latency WAN environments.

Fast smart cards are supported on Windows VDA only.

To enable fast smart card logon on Citrix Workspace app:

Fast smart card logon is enabled by default on the VDA and disabled by default on Citrix Workspace app. To enable fast smart card logon, include the following parameter in the `default.ica` file of the associated StoreFront site:

```
copy[WFClient]

SmartCardCryptographicRedirection=On
```

To disable fast smart card logon on Citrix Workspace app:

To disable fast smart card logon on Citrix Workspace app, remove the `SmartCardCryptographicRedirection` parameter from the `default.ica` file of the associated StoreFront site.

For more information, see smart-cards.

Silent authentication for Citrix Workspace

Citrix Workspace app introduces a Group Policy Object (GPO) policy to enable silent authentication for Citrix Workspace. This policy enables Citrix Workspace app to log in to Citrix Workspace automatically at system startup. Use this policy only when domain pass-through (single sign-on or SSON) is configured for Citrix Workspace on domain-joined devices. This feature is available from Citrix Workspace app for Windows version 2012 and later.

Starting with Citrix Workspace app for Windows version 2503, the system installs SSON by default in dormant mode. You can enable SSON post-installation using the Group Policy Object (GPO) policy. To enable, navigate to **User Authentication > Local user name and password** and select the **Enable pass-through authentication** checkbox.

> **Note:**
>
> You must reboot the system after updating the GPO policy for the SSON setting to take effect
>
> For this policy to function, the following criteria must be met:

- Single sign-on must be enabled.
- The `SelfServiceMode` key must be set to `Off` in the Registry editor.

Enabling silent authentication:

1. Open the Citrix Workspace app Group Policy Object administrative template by running `gpedit.msc`.
2. Under the **Computer Configuration** node, go to **Administrative Templates** > **Citrix Workspace** > **Self Service**.
3. Click the **Silent authentication for Citrix Workspace** policy and set it to **Enabled**.
4. Click **Apply** and **OK**.

Prevent Citrix Workspace app for Windows from caching passwords and usernames

By default, Citrix Workspace app for Windows automatically populates the last user name entered. To clear autofill of the user name field, edit the registry on the user device:

1. Create a REG_SZ value HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\AuthManager\RememberUsername.
2. Set its value false.

To disable the **Remember my password** check box and prevent an automatic sign-in, create following registry key on client machine where Citrix Workspace app for Windows is installed:

- Path: HKEY_LOCAL_MACHINE\Software\wow6432node\Citrix\AuthManager
- Type: REG_SZ

- Name: SavePasswordMode
- Value: Never

> **Note:**
>
> 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. Make sure you back up the registry before you edit it.

> To prevent caching credentials for the StoreFront stores, see Prevent Citrix Workspace app for Windows from caching passwords and usernames in the StoreFront documentation.

Support for more than 200 groups in Azure AD

With this release, an Azure AD user who is part of more than 200 groups can view apps and desktops assigned to the user. Previously, the same user wasn’t able to view these apps and desktops.

> **Note:**
>
> Users must sign out from Citrix Workspace app and sign in back to enable this feature.

Proxy authentication support

Previously, on client machines configured with proxy authentication, if the proxy credentials don't exist in the **Windows Credential Manager**, you aren't allowed to authenticate to Citrix Workspace app.

From Citrix Workspace app for Windows version 2102 and later, on client machines configured for proxy authentication, if the proxy credentials aren't stored in the **Windows Credential Manager**, an authentication prompt appears, asking you to enter the proxy credentials. Citrix Workspace app then saves the proxy server credentials in **Windows Credential Manager**. This results in a seamless login experience because you don't need to manually save your credentials in Windows Credential Manager before accessing Citrix Workspace app.

Always prompt end users for their credentials

Starting from 2212 version, Citrix Workspace app honors the setting Always prompt end users for their credentials.

User-Agent

Citrix Workspace app sends a user agent in network requests that can be used to configure authentication policies including redirection of authentication to other Identity Providers (IdPs).

> **Note:**
>
> The version numbers mentioned as part of the User-Agent in the following table are examples and it is automatically updated based on the versions that you are using.

> The following table describes the scenario, description, and the corresponding User-Agent for each scenario:

SCENARIO	DESCRIPTION	USER-AGENT
Regular HTTP requests	In general, a network request made by Citrix Workspace app contains a User-Agent. For example, network requests like: `GET /Citrix/Roaming/Accounts` and `GET / AGServices/discover`	`CitrixReceiver/23.5.0.63 Windows/10.0 (22H2 Build 19045.2965) SelfService/23.5.0.63 (Release) X1Class CWACapable`
Cloud store	When a user authenticates to a cloud store in Citrix Workspace app, network requests are made with a specific User-Agent. For example, network requests with path `/core/connect/authorize`.	`Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/113.0.0.0 Safari/537.36 Edg/113.0.1774.50 CWA/23.5.0.63 Windows/10.0 (22H2 Build 19045.2965)`

SCENARIO	DESCRIPTION	USER-AGENT
On-premises store with Gateway Advanced Auth using Edge WebView	When a user authenticates to the Gateway configured with Advanced Auth on Citrix Workspace app using Edge WebView, network requests are made with a specific User-Agent. For example, network requests that include: `GET /nf/auth/doWebview.do` and `GET /logon/LogonPoint/tmindex.html`.	`Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/108.0.0.0 Safari/537.36 Edg/108.0.1462.54 CWAWEBVIEW/23.2.0.2111 Windows/10.0 (22H2 Build 19045.2364)`
On-premises store with Gateway Advanced Auth using IE WebView	When a user authenticates to the Gateway configured with Advanced Auth on Citrix Workspace app using Internet Explorer WebView, network requests are made with a specific User-Agent. For example, network requests that include: `GET /nf/auth/doWebview.do` and `GET /logon/LogonPoint/tmindex.html`.	`Mozilla/5.0 (Windows NT 10.0; WOW64; Trident/7.0; rv:11.0) like Gecko, CWAWEBVIEW/23.5.0.43`
Custom web store	When a user adds a custom web store to Citrix Workspace app, the app sends a User-Agent.	`Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/113.0.0.0 Safari/537.36 Edg/113.0.1774.50 CWA/23.5.0.63 Windows/10.0 (22H2 Build 19045.2965)`

Domain pass-through access matrix

If you are using Citrix Workspace and want to achieve domain pass-through, the tables in the sub-sections describe the different scenarios and whether you can achieve domain pass-through for each scenario or not.

The different header elements in the tables and the additional information about the header elements are as follows:

- End Point joined to: Indicates the directory to which the endpoint is joined. The directory provides access control to on-premises resources. This can be on-premises Active Directory (AD), Azure Active Directory (AAD) or hybrid.
- Identity Provider (IdP): Entity used to provide authentication services to Citrix Workspace. It allows you to connect to the resources.
- Federated Authentication Service (FAS): For more information, see Enable single sign-on for workspaces with Citrix Federated Authentication Service.
- Virtual Delivery Agent (VDA): For more information, see Install VDAs.
- VDA Joined to: Indicates the directory to which the VDA device is joined. For more information, see Identity and access management.
- Single sign-on (SSO) to Citrix Workspace/VDA: Yes or No value indicates if domain pass-through to Citrix Workspace or VDA is supported.
- Citrix Workspace app: To achieve single sign-on, see Configure single sign-on during fresh installation in Domain pass-through authentication or Enhanced domain pass-through for single sign-on.

> **Note:**
>
> You might require latest version of Citrix Workspace app to get domain pass-through support for some of the following scenarios.

Domain pass-through support for Citrix Workspace

END POINT JOINED TO	IDP	VDA JOINED TO	SSO TO CITRIX WORKSPACE	SSO TO VDA	DOCUMENTATION
AD	On-premises Citrix Gateway	AD	Yes	Citrix Workspace app/FAS	Domain pass-through to Citrix Workspace using on-premises Citrix Gateway as the identity provider.
AD	Adaptive Authentication	AD	Yes	Citrix Workspace app/FAS	To configure adaptive authentication, see Adaptive Authentication service and follow the instruction in Domain pass-through to Citrix Workspace using on-premises Citrix Gateway as the identity provider.
AD	Citrix Gateway federated to	AD	Yes	Citrix Workspace app/FAS	Configure IdP using Configure

END POINT JOINED TO	IDP	VDA JOINED TO	SSO TO CITRIX WORKSPACE	SSO TO VDA	DOCUMENTATION
	another IdP (AAD/Okta)				SAML single sign-on and refer to the documentation for the IdP used to configure domain pass-through.
AD	Okta	AD	Yes	Citrix Workspace app/FAS	Domain pass-through to Citrix Workspace using Okta as identity provider.
AD/Hybrid Joined	AAD (AD with AAD Connect)	AD	Yes	Citrix Workspace app/FAS **	Domain pass-through to Citrix Workspace using Azure Active Directory as the identity provider.
AD	Any SAML based IdP (ex ADFS)	AD	Yes	Citrix Workspace app/FAS	See Connect SAML as an identity provider to Citrix Cloud and refer to the

END POINT JOINED TO	IDP	VDA JOINED TO	SSO TO CITRIX WORKSPACE	SSO TO VDA	DOCUMENTATION
					documentation for the IdP used to configure the domain pass-through.
AD	AD	AD	No	Not supported	NA
AD	AD+OTP	AD	No	Not supported	NA
AD	AAD	AAD	No	Not supported	NA
AAD	AAD without on-premises AD	AD	Yes	FAS	Citrix Workspace uses Microsoft Edge WebView which allows SSO to workspace. SSO to VDA is supported via FAS. For more information, see Enable single sign-on for workspaces with Citrix Federated

END POINT JOINED TO	IDP	VDA JOINED TO	SSO TO CITRIX WORKSPACE	SSO TO VDA	DOCUMENTATION
					Authentication Service.
AAD	AAD	AAD	Yes	User must enter credentials.	Citrix Workspace uses Microsoft Edge WebView which allows SSO to Workspace. SSO to VDA isn't supported.
Non-Domain Joined	IdP that supports password less authentication - link	AD	No	FAS	Citrix Workspace uses Microsoft Edge WebView which allows SSO to Workspace. SSO to VDA is supported via FAS. For more information, see Other ways to authenticate to Citrix Workspace.

Notes:

- Client must be reachable to AD for Kerberos to work.
- **Citrix Single Sign-on (SSONSVR.exe) works only with the user name or password on the client. If the user is using Windows Hello to sign in, then FAS is required or use Enhanced domain pass-through for single sign-on.
- Authentication might not be fully silent in cloud if LLT is enabled or if the end user acceptance policy is configured.
- It is recommended to configure FAS as it applies to non-windows platforms.

Starting with Citrix Workspace™ app for Windows version 2503, the system installs SSON by default in dormant mode. You can enable SSON post-installation using the Group Policy Object (GPO) policy. To enable, navigate to **User Authentication > Local user name and password** and select the **Enable pass-through authentication** checkbox.

Note:

You must reboot the system after updating the GPO policy for the SSON setting to take effect.

Domain pass-through support for StoreFront

END POINT JOINED TO	IDP	VDA JOINED TO	SSO TO CITRIX WORKSPACE	SSO TO VDA	DOCUMENTATION
AD	StoreFront	AD	Yes	Citrix Workspace app/FAS	Domain pass-through authentication
AD/Hybrid joined/ Windows Hello for Business	StoreFront	AD	Yes(1)	Citrix Workspace app /FAS(2)	Domain pass-through authentication and Enable

END POINT JOINED TO	IDP	VDA JOINED TO	SSO TO CITRIX WORKSPACE	SSO TO VDA	DOCUMENTATION
					single sign-on for workspaces with Citrix Federated Authentication Service.
AD	Citrix Gateway - Advanced Authentication	AD	Yes	Citrix Workspace app/FAS(3))	
AD	Citrix Gateway - Basic authentication	AD	Yes	Citrix Workspace app(4)	Domain pass-through authentication.

Notes:

1. Use Enhanced domain pass-through for single sign-on or in the Registry editor, navigate to the following path and set the `SSONCheckEnabled` string to `False` if you have not installed the single sign-on component.

   `HKEY_LOCAL_MACHINE\Software{Wow6432}\Citrix\AuthManager\protocols\integratedwindows\`

   The key prevents the Citrix Workspace app authentication manager from checking for the single sign-on component and allows Citrix Workspace app to authenticate to StoreFront.
2. If you are using Windows Hello to sign in, FAS is required and registry configuration to enable SSO.
3. Needs client to be reachable to AD as it uses Kerberos.
4. Works even if client is not reachable to AD. Not using Kerberos.

Domain pass-through to Citrix Workspace using on-premises Citrix Gateway as the identity provider

Important:

This article helps in configuring domain pass-through authentication. If you have already setup on-premises Gateway as IdP, skip to Configure domain pass-through as the authentication method in the Citrix Gateway section.

Citrix Cloud™ supports using an on-premises Citrix Gateway as an identity provider to authenticate subscribers signing into their workspaces.

By using Citrix Gateway authentication, you can:

- Continue authenticating users through your existing Citrix Gateway so they can access the resources in your on-premises Virtual Apps and Desktops deployment through Citrix Workspace.
- Use the Citrix Gateway authentication, authorization, and auditing functions with Citrix Workspace.
- Provide your users access to the resources that they need through Citrix Workspace using features such as pass-through authentication, smart cards, secure tokens, conditional access policies, federation.

Citrix Gateway authentication is supported for use with the following product versions:

- Citrix Gateway 13.1.4.43 Advanced edition or later

Prerequisites:

- Cloud Connectors - You need at least two servers on which to install the Citrix Cloud Connector™ software.
- An Active Directory and make sure that the domain is registered.
- Citrix Gateway requirements
    - Use advanced policies on the on-premises gateway because of the deprecation of classic policies.
    - When configuring the Gateway for authenticating subscribers to Citrix Workspace, the gateway acts as an OpenID Connect provider. Messages between Citrix Cloud and

Gateway conform to the OIDC protocol, which involves digitally signing tokens. Therefore, you must configure a certificate for signing these tokens.

- Clock synchronization – Citrix Gateway must be synchronized to NTP time.

For details, see Prerequisites in the Citrix Cloud documentation.

Before creating the OAuth IdP policy, you need to first set up Citrix Workspace or Cloud to use Gateway as the authentication option in the IdP. For details on how to set up, see Connect an on-premises Citrix Gateway to Citrix Cloud. When you complete the setup, the Client ID, Secret, and Redirect URL required for creating the OAuth IdP policy are generated.

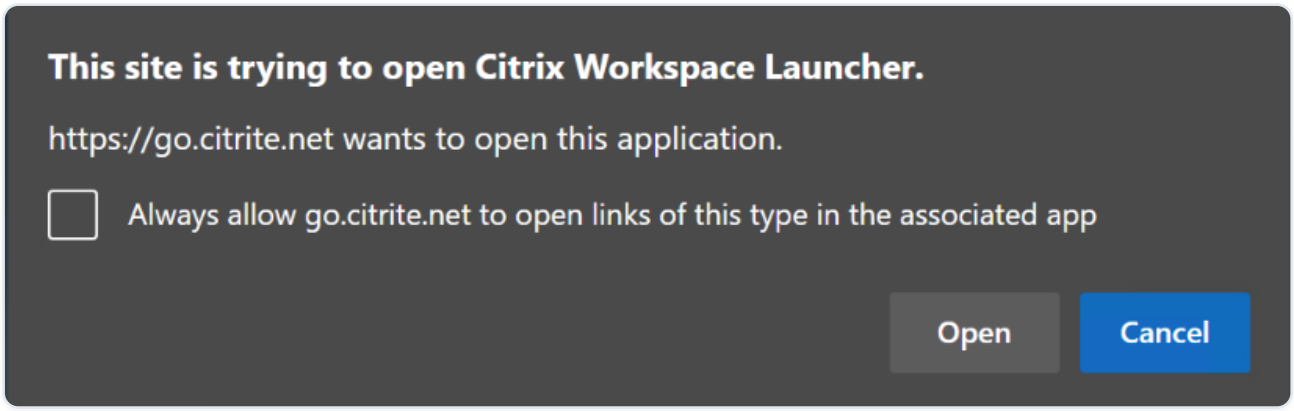
Domain pass-through for Workspace for web is enabled if you are using Internet Explorer, Microsoft Edge, Mozilla Firefox, and Google Chrome. Domain pass-through is enabled only when the client is detected successfully.

> **Note:**
>
> If HTML5 client is preferred by a user or is enforced by the administrator, domain pass-through authentication method is not enabled.
>
> When launching StoreFront URL in a browser, the **Detect Receiver** prompt is shown.

If the devices are managed, configure the group policy to disable this prompt instead of disabling client detection. For more information, see:

- URLAllowlist in the Microsoft documentation.
- URLAllowlist in the Google Chrome documentation.

> **Note:**
>
> Protocol handler used by Citrix Workspace app is **receiver:**. Configure this as one of the URLs allowed.
>
> Users can also select the check box as shown in the following example prompt for a StoreFront URL in the client detection prompt. Selecting this check box also avoids the prompt for subsequent launches.



The following steps explain how Citrix Gateway can be set up as IdP.

Create an OAuth IdP policy on the on-premises Citrix Gateway

Creating an OAuth IdP authentication policy involves the following tasks:

1. Create an OAuth IdP profile.
2. Add an OAuth IdP policy.
3. Bind the OAuth IdP policy to a virtual server.
4. Bind the certificate globally.

Create an OAuth IdP profile

1. To create an OAuth IdP profile by using the CLI, type the following in the command prompt:

```
add authentication OAuthIdPProfile <name> [-clientID <string>][-
clientSecret ][-redirectURL <URL>][-issuer <string>][-audience
<string>][-skewTime <mins>] [-defaultAuthenticationGroup <string>]



add authentication OAuthIdPPolicy <name> -rule <expression> [-action
<string> [-undefAction <string>] [-comment <string>][-logAction
<string>]



add authentication ldapAction <name> -serverIP <IP> -ldapBase
"dc=aaa,dc=local"



ldapBindDn <administrator@aaa.local> -ldapBindDnPassword <password>
-ldapLoginName sAMAccountName
```

```
add authentication policy <name> -rule <expression> -action <string>

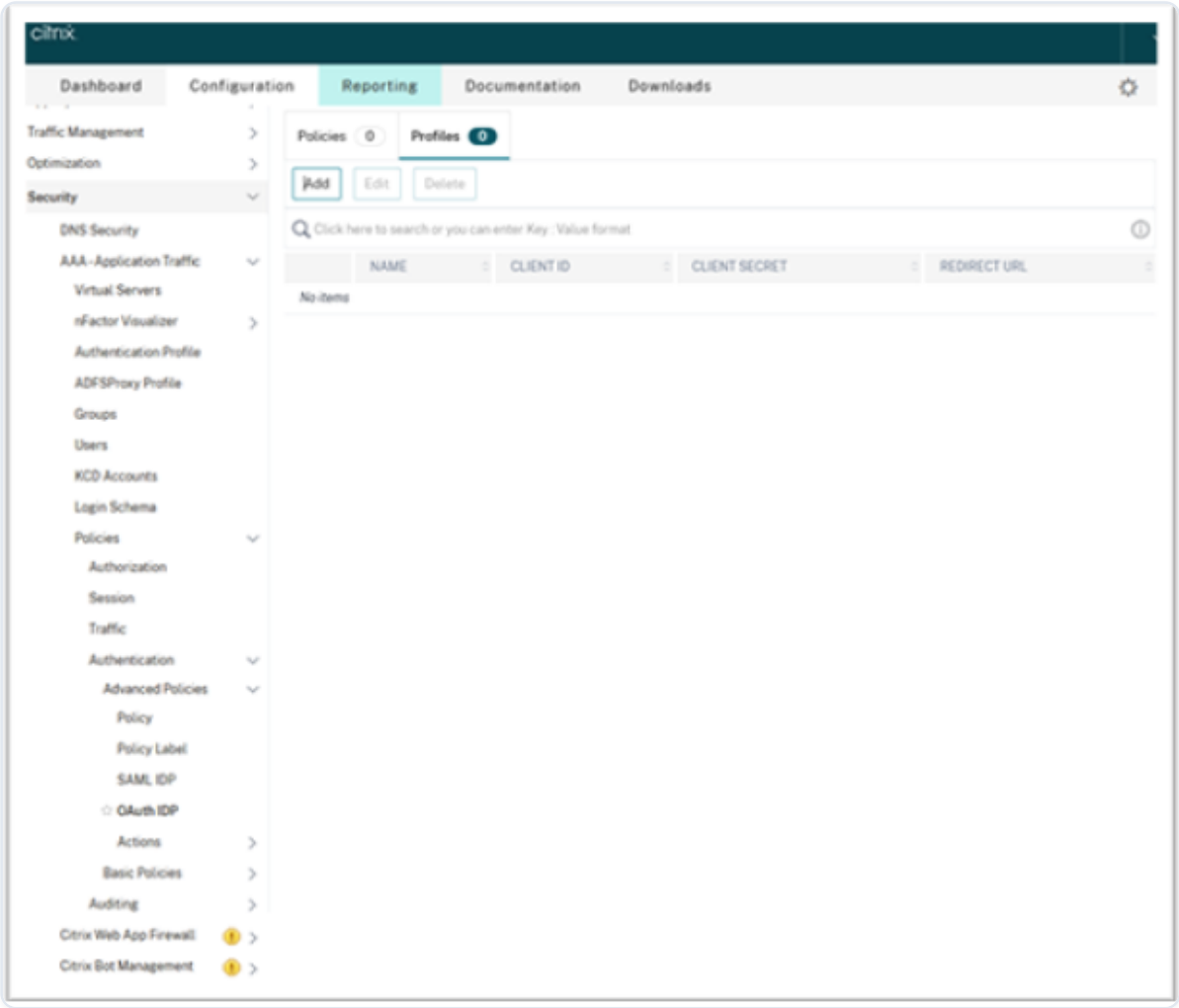

bind authentication vserver auth_vs -policy <ldap_policy_name>
-priority <integer> -gotoPriorityExpression NEXT


bind authentication vserver auth_vs -policy <OAuthIdPPolicyName>
-priority <integer> -gotoPriorityExpression END


bind vpn global –certkey <>
```

2. To create an OAuth IdP profile by using the GUI:

    a. Log into your on-premises Citrix Gateway management portal and navigate to **Security** > **AAA – Application Traffic** > **Policies** > **Authentication** > **Advanced Policies** > **OAuth IDP**.



b. In the **OAuth IdP** page, click the **Profiles** tab and click **Add**.

c. Configure the OAuth IdP profile.

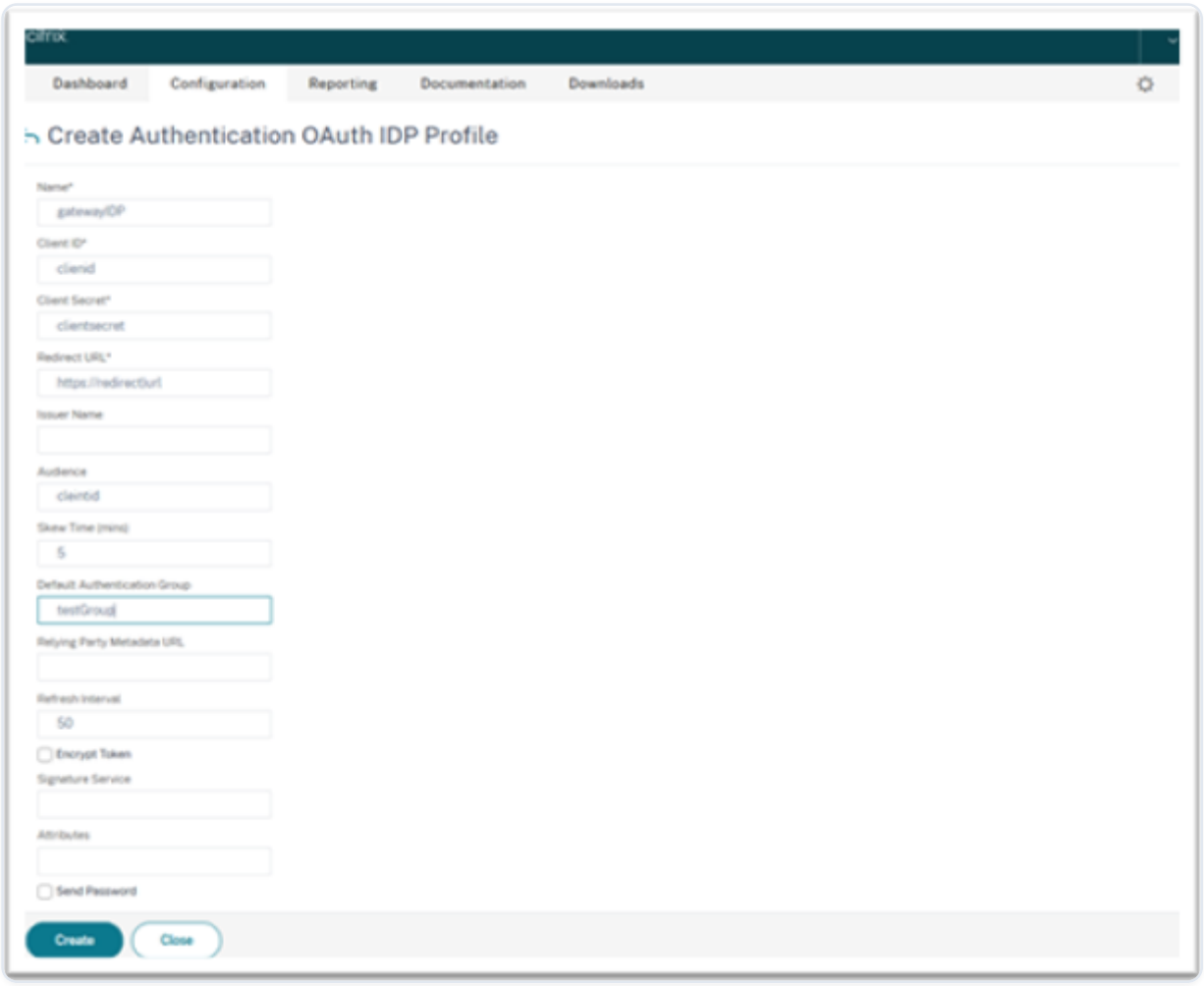
Note:

- Copy and paste the Client ID, Secret, and Redirect URL values from the **Citrix Cloud** > **Identity and Access Management** > **Authentication** tab to establish the connection to Citrix Cloud.
- Enter the Gateway URL correctly in the **Issuer Name** field. For example, `https://GatewayFQDN.com`.
- Also copy and paste the client ID in the **Audience** field.
- **Send Password**: Enable this option for single sign-on support. This option is disabled by default.

d. On the **Create Authentication OAuth IdP Profile** screen, set values for the following parameters and click **Create**.

- **Name** – Name of the authentication profile. Must begin with a letter, number, or the underscore character (_). Name must have only letters, numbers, and the hyphen (-), period (.) pound (#), space ( ), at (@), equals (=), colon (:), and underscore characters. You cannot change the name after the profile is created.
- **Client ID** – Unique string that identifies SP. Authorization server infers client configuration using this ID. Maximum Length: 127.
- **Client Secret** – Secret string established by user and authorization server. Maximum Length: 239.
- **Redirect URL** – Endpoint on SP to which code/token must be posted.
- **Issuer Name** – Identity of the server whose tokens are to be accepted. Maximum Length: 127. Example: `https://GatewayFQDN.com`.
- **Audience** – Target recipient for the token sent by IdP. The recipient verifies this token.
- **Skew Time** – This option specifies the allowed clock skew (in minutes) that Citrix ADC allows on an incoming token. For example, if skewTime is 10 then the token is valid from (current time - 10) mins to (current time + 10) mins, that is 20 mins in all. Default value: 5.
- **Default Authentication Group** – A group added to the session internal group list when this profile is chosen by IdP which can be used in the nFactor flow. It can be used in the expression (AAA.USER.IS_MEMBER_OF(“xxx”)) for authentication policies to identify relying party related nFactor flow. Maximum Length: 63

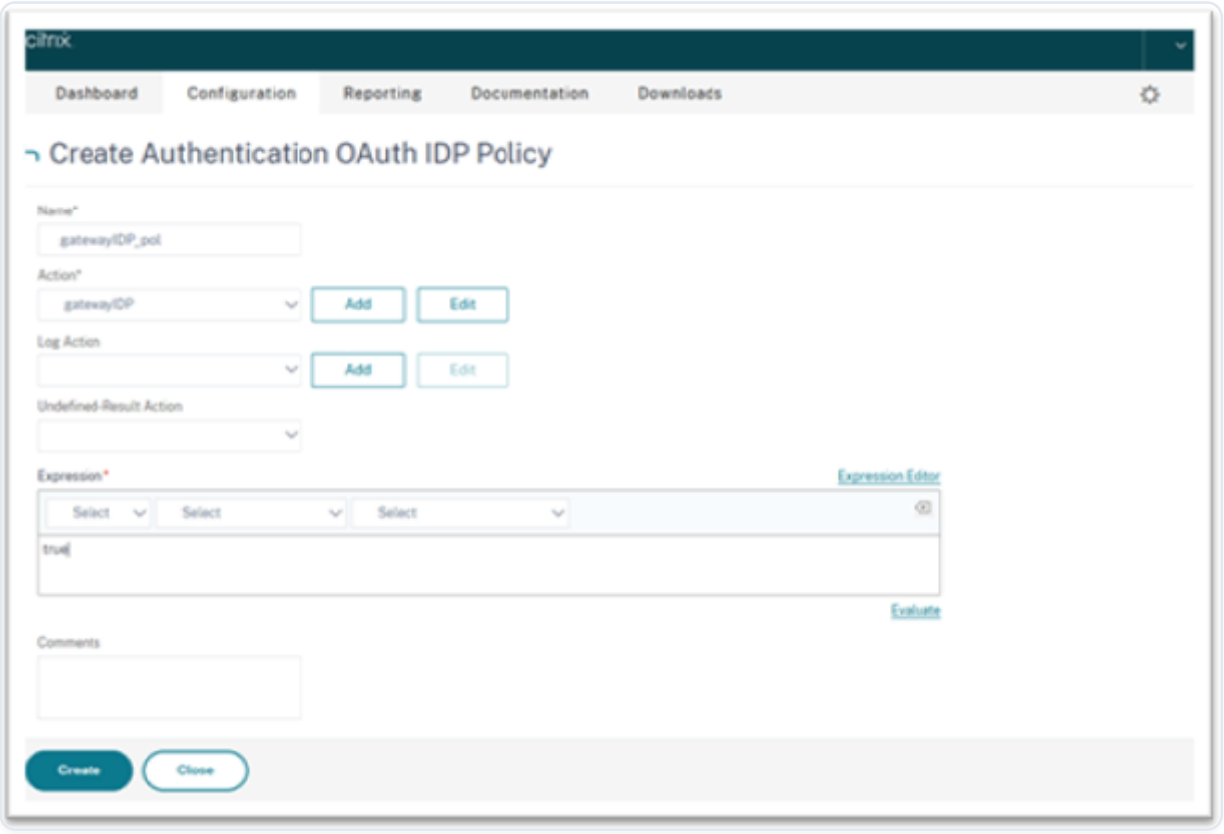
A group is added to the session for this profile to simplify policy evaluation and help in customizing policies. This group is the default group that is chosen when the authentication succeeds in addition to the extracted groups. Maximum Length: 63.



Add an OAuth IdP policy

1. In the OAuth IdP page, click **Policies** and click **Add**.
2. On the **Create Authentication OAuth IdP Policy** screen, set values for the following parameters and click **Create**.

   - **Name** – The name of the authentication policy.
   - **Action** – Name of profile created earlier.
   - **Log Action** – Name of the message log action to use when a request matches this policy. Not a mandatory filed.
   - **Undefined-Result Action** – Action to perform if the result of policy evaluation is undefined (UNDEF). Not a mandatory field.
   - **Expression** – Default syntax expression that the policy uses to respond to specific request. For example, true.
   - **Comments** – Any comments about the policy.



> **Note:**
>
> When sendPassword is set to ON (OFF by default), user credentials are encrypted and passed through a secure channel to Citrix Cloud. Passing user credentials through a secure channel allows you to enable SSO to Citrix Virtual Apps and Desktops™ upon launch.

Bind the OAuthIDP policy and LDAP policy to the virtual authentication server

Now you need to bind the OAuth IdP Policy to the virtual authentication server on the on-premises Citrix Gateway.

1. Log into your on-premises Citrix Gateway management portal and navigate to **Configuration** > **Security** > **AAA-Application Traffic** > **Policies** > **Authentication** > **Advanced Policies** > **Actions** > **LDAP**.
2. On the **LDAP Actions** screen, click **Add**.
3. On the Create Authentication LDAP Server screen, set the values for the following parameters, and click **Create**.

    - **Name** – The name of the LDAP action.

- **ServerName/ServerIP** – Provide FQDN or IP of the LDAP server.
- Choose appropriate values for **Security Type**, **Port**, **Server Type**, **Time-Out**.
- Make sure that **Authentication** is checked.
- **Base DN** – Base from which to start LDAP search. For example, `dc=aaa`, `dc=local`.
- **Administrator Bind DN**: User name of the bind to LDAP server. For example, `admin@aaa.local`.
- **Administrator Password/Confirm Password**: Password to bind LDAP.
- Click **Test Connection** to test your settings.
- **Server Logon Name Attribute**: Choose "sAMAccountName".
- Other fields are not mandatory and hence can be configured as required.

4. Navigate to **Configuration** > **Security** > **AAA-Application Traffic** > **Policies** > **Authentication** > **Advanced Policies** > **Policy**.
5. On the **Authentication Policies** screen, click **Add**.
6. On the **Create Authentication Policy** page, set the values for the following parameters, and click **Create**.

   - **Name** – Name of the LDAP Authentication Policy.
   - **Action Type** – Choose LDAP.
   - **Action** – Choose the LDAP action.
   - **Expression** – Default syntax expression that the policy uses to respond to specific request. For example, true**.

Bind the certificate globally to the VPN

Binding the certificate globally to the VPN requires CLI access to the on-premises Citrix Gateway. Using Putty (or similar) login to the on-premises Citrix Gateway using SSH.

1. Launch a command-line utility, such as, Putty.
2. Sign in to the on-premises Citrix Gateway using SSH.
3. Type the following command: `show vpn global`

> **Note:**
>
> No certificate must be bound.

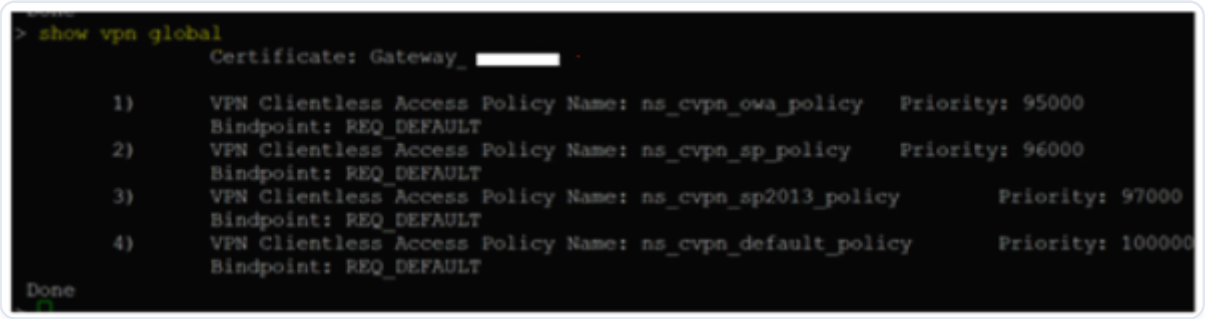


4. To list the certificates on the on-premises Citrix Gateway, type the following command: `show ssl certkey`
5. Select the appropriate certificate and type the following command to bind the certificate globally to VPN:

   `bind vpn global -certkey cert_key_name`

   where cert_key_name is the name of the certificate.
6. Type the following command to check if the certificate is bound globally to the VPN:

   `show vpn global`



Configure domain pass-through as the authentication method in the Citrix Gateway

When you complete setting up the Citrix Gateway as IdP, perform the following steps to configure the domain pass-through as the authentication method in the Citrix Gateway.

When the domain pass-through is set as the authentication method, the client uses Kerberos tickets to authenticate instead of credentials. Citrix Gateway supports both Impersonation and Kerberos Constrained Delegation (KCD). However, this article describes KCD authentication. For more information, see Knowledge Center article CTX236593.

Configuring the domain pass-through includes the following steps:

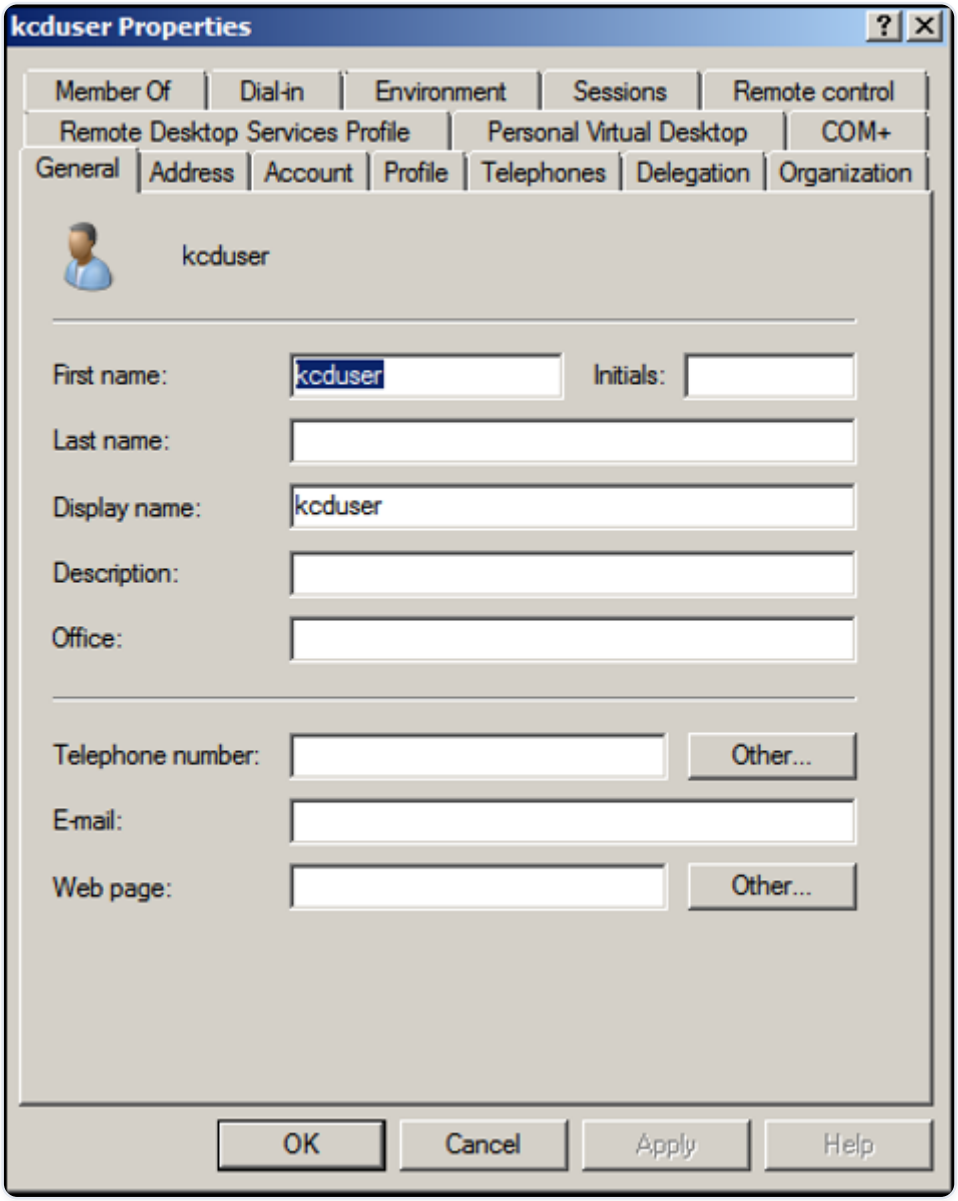
1. Kerberos Constrained Delegation configuration
2. Client configuration

Kerberos Constrained Delegation configuration

1. Create a KCD user in the Active Directory

   Kerberos works on a ticket granting system to authenticate users to resources, and involves a client, server, and Key Distribution Center (KDC).

   For Kerberos to work, the client needs to request a ticket from the KDC. The client must first authenticate to the KDC using their user name, password, and domain before requesting a ticket, called as AS request.



2. Associate the new user with the Service Principal Name (SPN).

   SPN of Gateway is used by the client to authenticate.

   - Service Principal Name (SPN): A Service Principal Name (SPN) is a unique identifier of a service instance. Kerberos authentication uses SPN to associate a service instance with a

service sign-in account. This function allows a client application to request for the service authentication of an account even if the client doesn't have the account name.

SetSPN is the application for managing SPNs on a Windows device. With SetSPN, you can view, edit, and delete SPN registrations.

a. In the Active Directory server, open a command prompt.
b. In the command prompt, enter the following command:

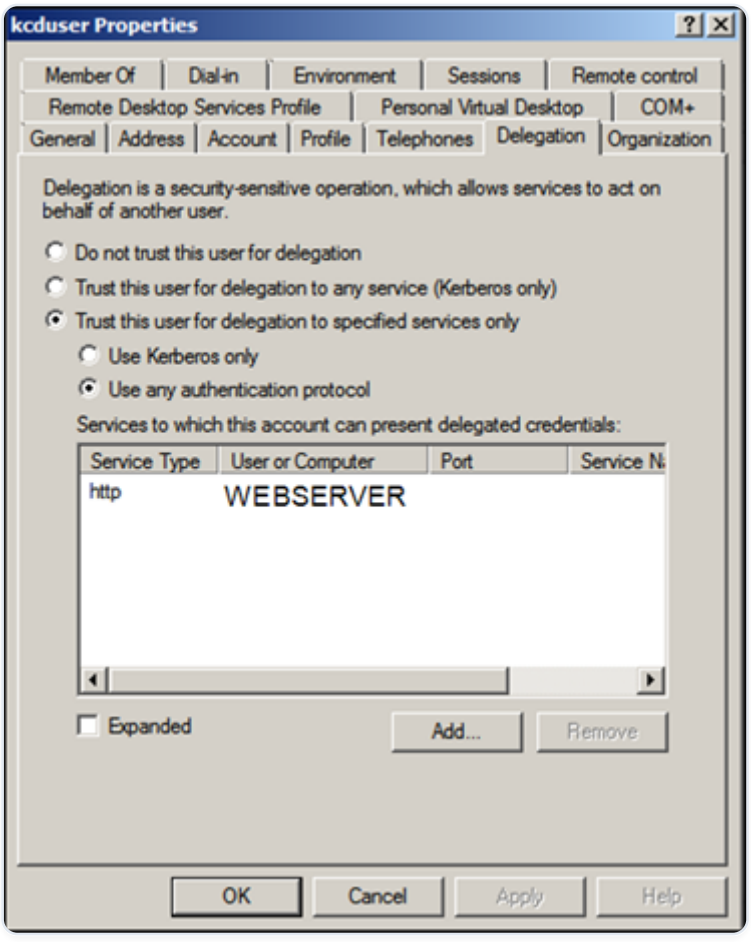
```
setspn –A http/<LB fqdn> <domain\Kerberos user>
```

c. To confirm the SPNs for the Kerberos user, run the following command:

```
setspn –l <Kerberos user>
```

The Delegation tab appears after running the `setspn` command.

d. Select **Trust this user for delegation to specified services only** option and **Use any authentication protocol** option. Add the web server and select the HTTP service.

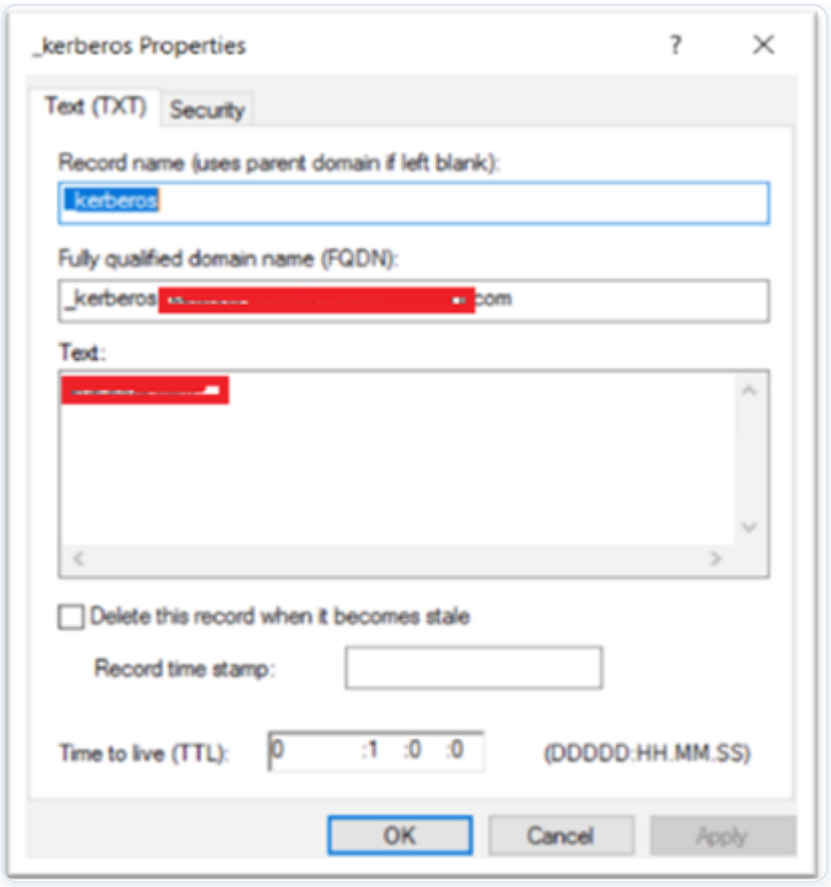


3. Create a DNS record for the client to find the Gateway's SPN:

Add a TXT DNS record in the Active Directory.

Note:

Name must start with _Kerberos, Data must be the domain name. The FQDN must show Kerberos.<domain_name>.



A window's domain joined client uses _kerberos.fqdn to request tickets. For example, if the client is joined to citrite.net, the operating system can get tickets for any websites with *.citrite.net. However, if the Gateway domain is external like gateway.citrix.com, then the client operating system can't get the Kerberos ticket.

Hence, you must create a DNS TXT record that helps the client to look up for the _kerberos.gateway.citrix.com and get the Kerberos ticket for authentication.

4. Configure Kerberos as the authentication factor.

   a. Create a KCD Account for the NetScaler® user. Here we opted to do this manually, but you can create a keytab file.

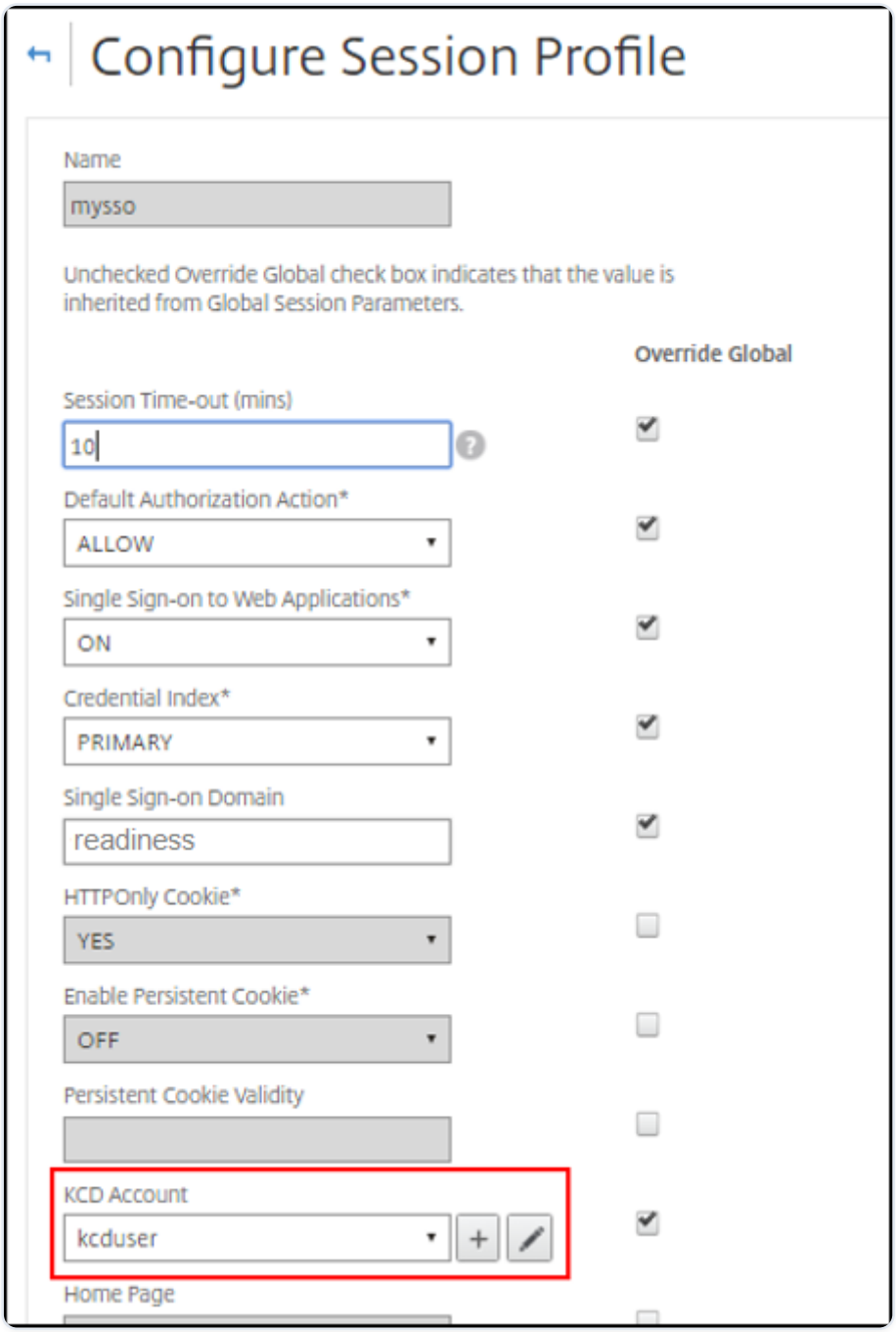
      Note:

> If you are using alternate domains (Internal domain and external domain) then you must set the Service SPN to `HTTP/PublicFQDN.com@InternalDomain.ext`.

- **Realm** - Kerberos Realm. Usually your Internal Domain suffix.
- **User Realm** - This is your user's Internal Domain suffix.
- **Enterprise Realm** - This needs to be given only in certain KDC deployments where KDC expects Enterprise user name instead of Principal Name.
- **Delegated User** - This is the NetScaler user account for KCD that you created in AD in the prior steps. Make sure that the password is correct.



b. Ensure that the Session Profile is using the right KCD account. Bind the session policy to the authentication, authorization, and auditing virtual server.



c. Bind the Authentication policy to the authentication, authorization, and auditing virtual server. These policies use authentication, authorization, and auditing methods that do not obtain a password from the client, hence the need to use KCD. However, they must still obtain the user name and domain information, in UPN format.

> **Note:**
>
> You can use IP address or EPA scan to differentiate domain joined and non-domain joined devices and use Kerberos or regular LDAP as a factor for authentication.

Configure the client

To allow successful single sign-on to VDA, perform the following.

Prerequisites:

- Domain joined machine
- Citrix Workspace 2112.1or later with SSO setting enabled
- Trust necessary URLs that checks if the connections are secured
- Validate Kerberos from Client and AD. Client OS must have connectivity to AD to get Kerberos tickets.

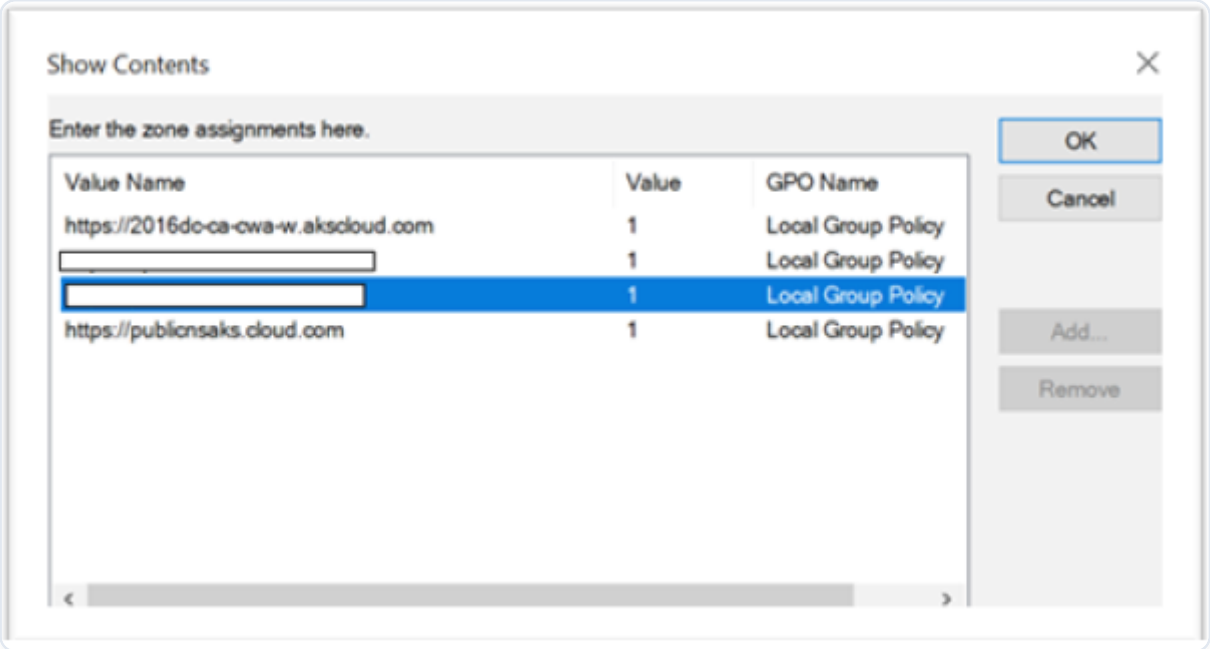
Following are some of the URLs to be trusted in the browser:

- Gateway URL or FQDN
- AD FQDN
- Cloud store URL for SSO from browser-based launches.

1. If you are using Internet Explorer, Microsoft Edge, or Google Chrome, do the following:

    a. Launch the browser.

    b. Open the Local Group Policy Editor on the Client.



    a. Go to **Computer Configuration** > **Windows Component** > **Internet Explorer** > **Internet Control Panel** > **Security** page.

    b. Open Site to zone Assignment list and add all the listed URLs with the Value one (1).

c. (Optional) Run `Gpupdate` to apply policies.

2. If you are using Mozilla Firefox browser, do the following:

   a. Open the browser.

   b. Type `about:config` in the search bar.

   c. Accept the risk and continue.

   d. In the search field, type **negotiate**.

   e. From the list of populated data, verify if the **network.negotiate-auth.trusted-uris** is set to the domain value.



   This completes the configuration on the client-side.

3. Login using Citrix Workspace app or browser to Workspace.

This must not prompt for user name or password on a domain joined device.

Troubleshooting Kerberos

> **Note:**
>
> You must be domain admin to run this verification step.
>
> In the command prompt or Windows PowerShell, run the following command to verify Kerberos ticket validation for the SPN user:

`KLIST get host/FQDN of AD`

Domain pass-through to Citrix Workspace using Azure Active Directory as the identity provider

You can implement single sign-on (SSO) to Citrix Workspace using Azure Active Directory (AAD) as an identity provider with Domain joined, Hybrid, and Azure AD enrolled endpoints/VMs.

With this configuration, you can also use Windows Hello to SSO to Citrix Workspace using AAD enrolled endpoints.

- You can authenticate to Citrix Workspace app using Windows Hello.
- FIDO2 based Authentication with the Citrix Workspace app.
- Single sign-on to Citrix Workspace app from Microsoft AAD joined machines (AAD as IdP) and conditional access with AAD.

To achieve SSO to virtual apps and desktops, you can either deploy FAS or configure Citrix Workspace app as follows.

> **Note:**

> You can achieve SSO to the Citrix Workspace resources only when using Windows Hello. However, you're prompted for user name and password when accessing your published virtual apps and desktops. To solve this prompt, you can deploy FAS and SSO to virtual apps and desktops.

> **Prerequisites:**

1. Connect Azure Active Directory to Citrix Cloud. For more information, see Connect Azure Active Directory to Citrix Cloud in the Citrix Cloud documentation.
2. Enable Azure AD authentication to access workspace. For more information, see Enable Azure AD authentication for workspaces in the Citrix Cloud documentation.

To achieve single sign-on to Citrix Workspace:

1. Configure Citrix Workspace app with includeSSON.
2. Disable `prompt=login` attribute in Citrix Cloud.
3. Configure Azure Active Directory pass-through with Azure Active Directory Connect.

Starting with Citrix Workspace™ app for Windows version 2503, the system installs SSON by default in dormant mode. You can enable SSON post-installation using the Group Policy Object (GPO) policy. To enable, navigate to **User Authentication > Local user name and password** and select the **Enable pass-through authentication** checkbox.

> **Note:**

> You must reboot the system after updating the GPO policy for the SSON setting to take effect.

Configure Citrix Workspace app to support SSO

Prerequisites:

- Citrix Workspace version 2109 or higher.

> **Note:**
>
> If you're using FAS for SSO, Citrix Workspace configuration isn't needed.

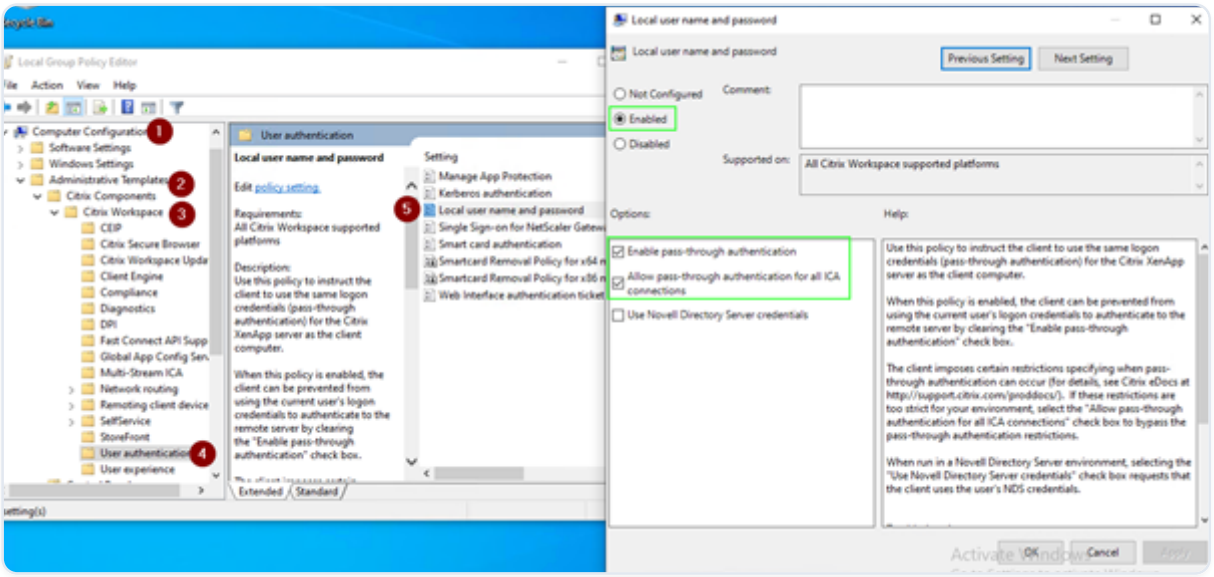
1. Install Citrix Workspace app from administrative command line with option `includeSSON`:

   `CitrixWorkspaceApp.exe /includeSSON`

2. Sign out from the Windows client and sign in to start the SSON server.
3. Click **Computer configuration** > **Administrative templates** > **Citrix Components** > **Citrix Workspace** > **User Authentication** to change Citrix Workspace GPO to allow **Local username and password**.

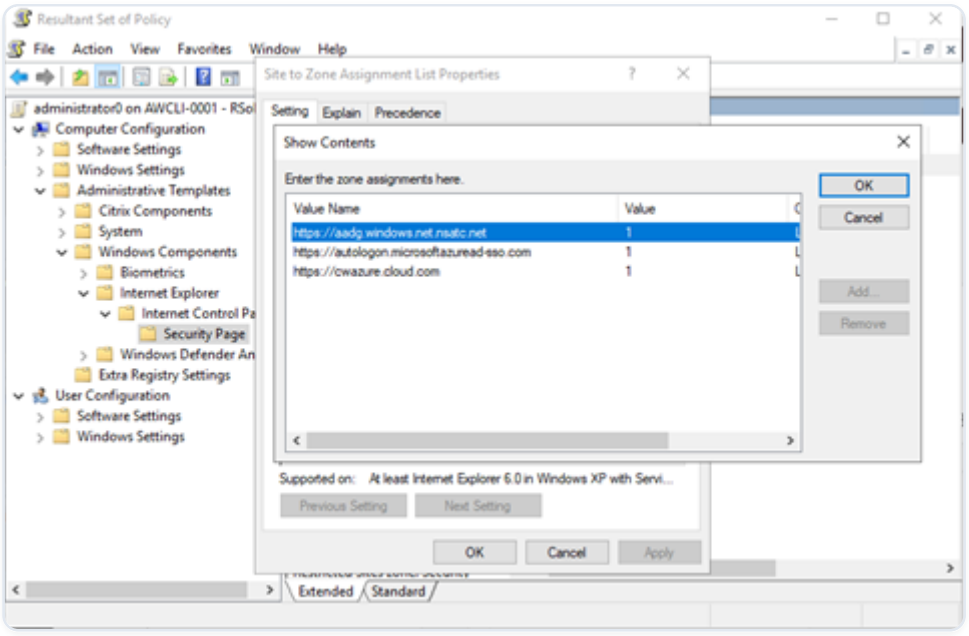
   > **Note:**
   >
   > These policies can be pushed to the client device via Active Directory. This step is required only when accessing Citrix Workspace from the web browser.

4. Enable the setting as per the screenshot.



5. Add the following trusted sites via GPO:

   - `https://aadg.windows.net.nsatc.net`
   - `https://autologon.microsoftazuread-sso.com`
   - `https://xxxtenantxxx.cloud.com`: cloud store URL



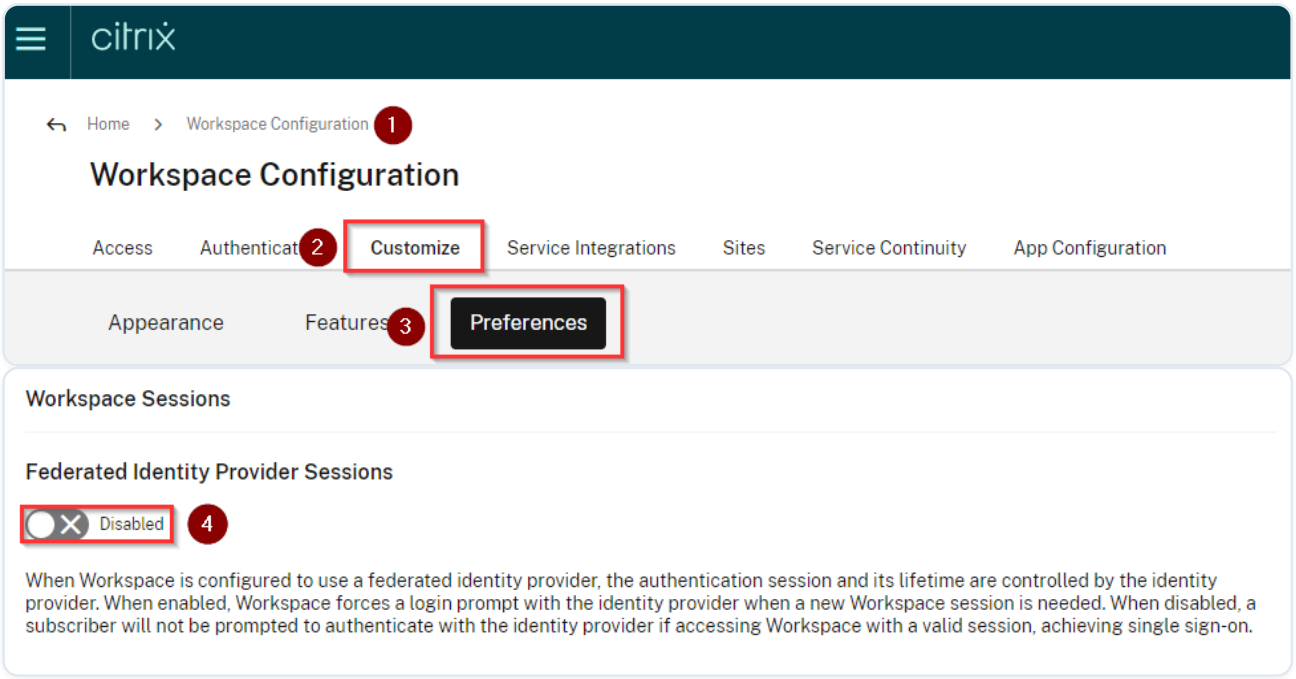
Note:

Single sign-on for AAD is disabled when the **AllowSSOForEdgeWebview** registry in `Computer\HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\Citrix\Dazzle` is set to false.

Disable prompt=login parameter in Citrix Cloud

By default `prompt=login` is enabled for Citrix Workspace that forces the authentication even if the user opted to **stay signed in** or if the device is Azure AD joined.

You can disable `prompt=login` in your Citrix Cloud account. Navigate to `StoreFront Cloud\Customize\Preferences-Federated Identity Provider Sessions` and disable the toggle. For more information, see Knowledge Center article CTX253779.



Note:

On AAD joined or hybrid AAD joined devices, if AAD is used as IdP for Workspace, then Citrix Workspace app doesn't prompt for credentials. Users can automatically sign in using work or school account.

To allow users to sign in using different account, set the following registry to false.

Create and add a registry string REG_SZ with the **AllowSSOForEdgeWebview** name under `Computer\HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\Citrix\Dazzle` or `Computer\HKEY_CURRENT_USER\SOFTWARE\Citrix\Dazzle` and set its value as False. Alternatively, if users sign out from Citrix Workspace app, users can sign in with a different account on the next sign-in.

Configure Azure Active Directory pass-through with Azure Active Directory Connect

- If you're installing Azure Active Directory Connect for the first time, on the **User sign-in** page, select **Pass-through Authentication** as the sign On method. For more information, see Azure Active Directory Pass-through Authentication: Quickstart in the Microsoft documentation.
- If Microsoft Azure Active Directory Connect exists:

  a. Select the **Change user sign-in** task and click **Next**.

  b. Select **Pass-through Authentication** as the sign-in method.

Note:

You can skip this step if the client device is Azure AD joined, or hybrid joined. If the device is AD joined, domain pass-through authentication works using kerberos authentication.

Domain pass-through to Citrix Workspace using Okta as identity provider

You can achieve single sign-on to Citrix Workspace using Okta as the identity provider (IdP).

Prerequisites:

- Citrix Cloud™
  - Cloud Connectors

  Note: If you're new to Citrix Cloud, define a Resource Location, and have the connectors configured. It's recommended to have at least two cloud connectors deployed in production environments. For information on how to install Citrix Cloud Connectors, see Cloud Connector Installation.

  - Citrix Workspace
  - Federated Authentication Service (optional). For more information, see Enable single sign-on for workspaces with Citrix Federated Authentication Service.
- Citrix DaaS (formerly Citrix Virtual Apps and Desktops™ Service)
- AD domain joined VDA or physical AD joined devices
- Okta Tenant

- Okta IWA Agent (Integrated Windows Authentication)
- Okta Verify (Okta Verify can be downloaded from the app store) (optional)

- Active Directory

1. Deploy the Okta AD Agent:
   a. In the Okta Admin portal, click **Directory** > **Directory Integrations**.
   b. Click **Add Directory** > **Add Active Directory**.
   c. Review the installation requirements by following the workflow, which covers the Agent Architecture and Installation Requirements.
   d. Click the **Set Up Active Directory** button and then click **Download Agent**.
   e. Install Okta AD Agent onto a Windows server by following the instruction provided in Install the Okta Active Directory agent.

   Note:

   Make sure that the prerequisites mentioned in Active Directory integration prerequisites are met before installing the agent.

2. Set up Integrated Windows Authentication (IWA):
   a. On the Okta Admin portal, click **Security** and then **Delegated Authentication**.
   b. Scroll down to the **On-prem Desktop SSO** part on the page that loads and click **Download Agent**.
   c. Set up the **Routing Rules** for IWA. For more information, see Configure Identity Provider routing rules.

3. Launch the Okta customer portal.

   Note:

   - When you install Okta IWA Agent and the status is enabled, you can sign in from a Windows Domain joined device. This configuration also jumps past the login and

directs you to the IWA login page and passes the user credentials.



- For more information on how to troubleshoot any issues, see Install and configure the Okta IWA Web agent for Desktop single sign-on.

4. Sign in to Citrix Cloud at `https://citrix.cloud.com` and enable Okta as the IdP. For information, see Tech Insight: Authentication - Okta in the Citrix Tech Zone documentation.

Note:

You can sign in from either the Citrix Workspace app or browser, both provides the pass-through experience as per the Tech Zone documentation.

5. To achieve SSO to virtual apps and desktops, you can either deploy FAS or configure the Citrix Workspace app.

Note:

Without FAS, you're prompted for the AD user name and password. For more information, see Enable single sign-on for workspaces with Citrix Federated Authentication Service. If you aren't using FAS, Configure Citrix Workspace app to support SSO.

Domain pass-through (single sign-on) authentication

Domain pass-through (single sign-on or SSON) also known as legacy domain pass-through (SSON)lets you authenticate to a domain and use Citrix Virtual Apps and Desktops™ and Citrix DaaS (formerly Citrix Virtual Apps and Desktops service) without having to reauthenticate again.

Note:

- The **Enable MPR notifications for the System** or **Configure the transmission of the user's password in the content of MPR notifications sent by Winlogon** policy in the Group Policy Object template must be enabled to support the domain pass-through (single sign-on) authentication feature on Windows 11. Depending on the 24H2 patch level, you can see either of the policy names. By default, this policy is disabled on Windows 11 24H2. So, if upgraded to Windows 11 24H2, you must enable the **Enable MPR notifications for the System** policy.
- This feature is available from Citrix Workspace app for Windows version 2012 and later.
- You can't use legacy domain pass-through (SSON) and enhanced domain pass-through together for authentication.

When enabled, domain pass-through (single sign-on) caches your credentials, so that you can connect to other Citrix® applications without having to sign in each time. Ensure that only software that is in accordance with your corporate policies runs on your device to mitigate the risk of credential compromise.

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

All web browsers require you to configure single sign-on using the Group Policy Object (GPO) administrative template. For more information about configuring single sign-on using the Group Policy Object (GPO) administrative template, see Configure single sign-on with Citrix Gateway.

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

- Command-line interface
- GUI

Note:

> The terms domain pass-through, single sign-on, and SSON might be used interchangeably in this document.

> Starting with Citrix Workspace™ app for Windows version 2503, the system installs SSON by default in dormant mode. You can enable SSON post-installation using the Group Policy Object (GPO) policy. To enable, navigate to **User Authentication > Local user name and password** and select the **Enable pass-through authentication** checkbox.

> **Note:**
>
> You must reboot the system after updating the GPO policy for the SSON setting to take effect.

> **Limitations:**

Domain pass-through using user credentials has the following limitations:

- Doesn't support passwordless authentication with modern authentication methods such as Windows Hello or FIDO2. An additional component called the Federated Authentication Service (FAS) is required for single sign-on (SSO).
- Installation or upgrade of Citrix Workspace app with SSON enabled requires a reboot of the device.
- Requires Multi Provider Router (MPR) notifications to be enabled on Windows 11 machines.
- Must be on the top of the list of network providers order.

To overcome the preceding limitations, use Enhanced domain pass-through for single sign-on (Enhanced SSO).

Configure single sign-on during fresh installation

To configure single sign-on during fresh installation, do the following steps:

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

Configure single sign-on on StoreFront

Single sign-on lets you authenticate to a domain and use Citrix Virtual Apps and Desktops and Citrix DaaS from the same domain without having to reauthenticate to each app or desktop.

When you add a store using the **Storebrowse** utility, your credentials pass through the Citrix Gateway server, along with the apps and desktops enumerated for you, including your Start menu settings. After configuring single sign-on, you can add the store, enumerate your apps and desktops, and launch the required resources without having to type your credentials multiple times.

Depending on the Citrix Virtual Apps and Desktops deployment, single sign-on authentication can be configured on StoreFront using the Management Console.

Use the following table for different use cases and its respective configuration:

USE CASE	CONFIGURATION DETAILS	ADDITIONAL INFORMATION
Configured SSON on StoreFront	Launch Citrix Studio, go to **Stores** > **Manage Authentication Methods - Store** > enable **Domain pass-through**.	When Citrix Workspace app isn't configured with single sign-on, it automatically switches the authentication method from **Domain pass-through** to **User name and password**, if available.
When workspace for web is required	Launch **Stores** > **Workspace for Web Sites** > **Manage Authentication Methods - Store** > enable **Domain pass-through**.	When Citrix Workspace app isn't configured with single sign-on, it automatically switches the authentication method from **Domain pass-through** to **User name and password**, if available.

Configure single sign-on with Citrix Gateway

You enable single sign-on with Citrix Gateway using the Group Policy Object administrative template. However, you must ensure that you have enabled basic authentication and single factor (nFactor with 1 Factor) authentication on the Citrix Gateway.

1. Open the Citrix Workspace app GPO administrative template by running `gpedit.msc`.
2. Under the **Computer Configuration node**, go to **Administrative Template** > **Citrix Components** > **Citrix Workspace** > **User Authentication**, and select **Single Sign-on for Citrix Gateway** policy.

3. Select **Enabled**.
4. Click **Apply** and **OK**.
5. Restart Citrix Workspace app for the changes to take effect.

Configure XML trust services on the Delivery Controller

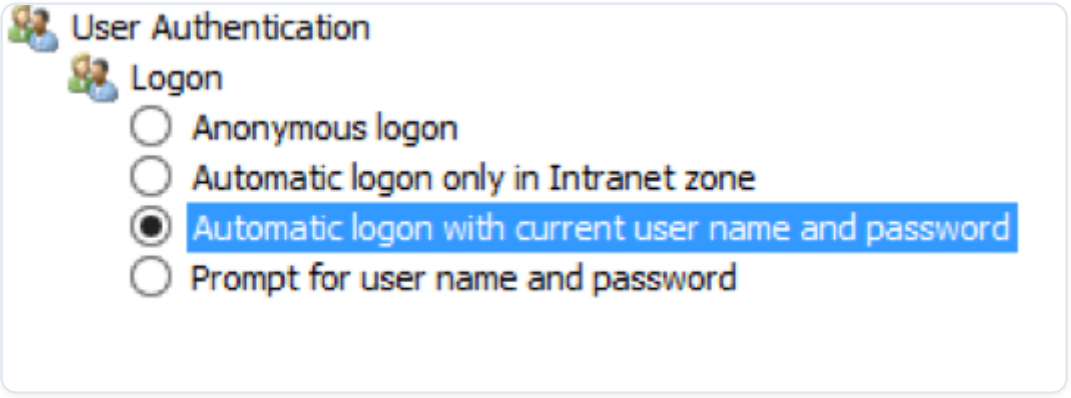
On Citrix Virtual Apps and Desktops and Citrix DaaS™, run the following PowerShell command as an administrator on the Delivery Controller:

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

Modify the Internet Explorer settings

1. Add the StoreFront server to the list of trusted sites using Internet Explorer. To add:
    a. Launch **Internet Options** from the Control panel.
    b. Click **Security** > **Local Intranet** and click **Sites**.

    The **Local Intranet** window appears.
    c. Select **Advanced**.
    d. Add the URL of the StoreFront FQDN with the appropriate HTTP or HTTPS protocols.
    e. Click **Apply** and **OK**.
2. Modify the **User Authentication** settings in **Internet Explorer**. To modify:
    a. Launch **Internet Options** from the Control panel.
    b. Click **Security** tab > **Local Intranet**.
    c. Click **Custom level**. The **Security Settings – Local Intranet Zone** window appears.
    d. In the **User Authentication** pane, select **Automatic logon with current user name and password**.



    e. Click **Apply** and **OK**.

Configure single sign-on using the command-line interface

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

Configure single sign-on using the GUI

1. Locate the Citrix Workspace app installation file (`CitrixWorkspaceApp.exe`).
2. Double-click `CitrixWorkspaceApp.exe` to launch the installer.
3. In the **Enable Single Sign-on installation** wizard, select the **Enable Single Sign-on** option.
4. Click **Next** and follow the prompts to complete the installation.

You can now log on to an existing store (or configure a new store) using Citrix Workspace app without entering user credentials.

Configure single sign-on on workspace for web

You can configure single sign-on on workspace for web using the Group Policy Object administrative template.

1. Open the workspace for web GPO administrative template by running gpedit.msc.
2. Under the **Computer Configuration** node, go to **Administrative Template** \> **Citrix Component** \> **Citrix Workspace** \> **User Authentication**.
3. Select the **Local user name and password** policy and set it to **Enabled**.
4. Click **Enable pass-through authentication**. This option allows the workspace for web to use your login credentials for authentication on the remote server.
5. Click **Allow pass-through authentication for all ICA® connections**. This option bypasses any authentication restriction and allows credentials to pass-through on all the connections.
6. Click **Apply** and **OK**.
7. Restart the workspace for web for the changes to take effect.

Verify that the single sign-on is enabled by launching the **Task Manager** and check if the `ssonsvr.exe` process is running.

Configure single sign-on using Active Directory

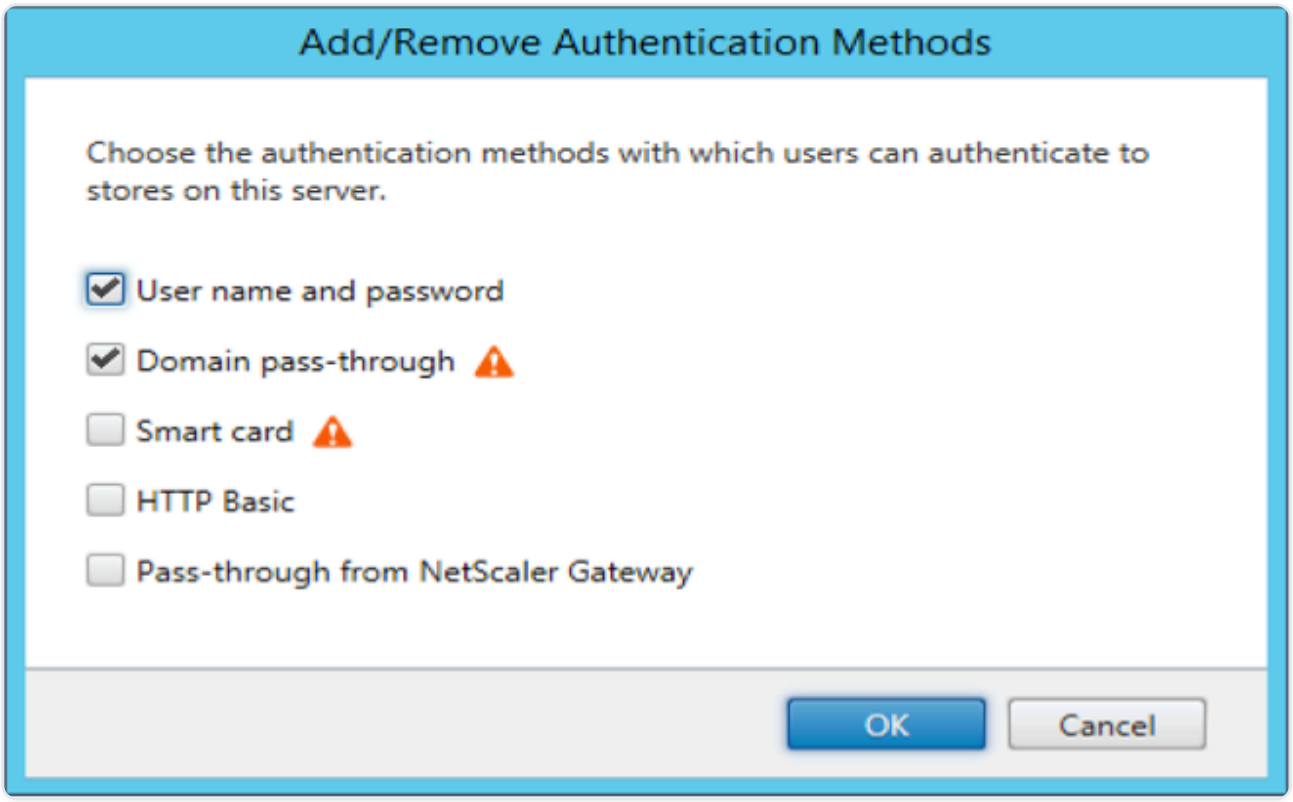
Complete the following steps to configure Citrix Workspace app for pass-through authentication using Active Directory group policy. In this scenario, you can achieve the single sign-on authentication without using the enterprise software deployment tools, such as the Microsoft System Center Configuration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

1. Download and place the Citrix Workspace app installation file (CitrixWorkspaceApp.exe) on a suitable network share. It must be accessible by the target machines you install Citrix Workspace app on.
2. Get the `CheckAndDeployWorkspacePerMachineStartupScript.bat` template from the Citrix Workspace app for Windows Download page.
3. Edit the content to reflect the location and the version of `CitrixWorkspaceApp.exe`.
4. In the **Active Directory Group Policy Management** console, type `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 `receiver.adml` file.
6. After adding the `receiver.adml` template, go to **Computer Configuration** > **Administrative Templates** > **Citrix Components** > **Citrix Workspace** > **User authentication**. For more information about adding the template files, see Group Policy Object administrative template.
7. Select the **Local user name and password** policy and set it to **Enabled**.
8. Select **Enable pass-through authentication** and click **Apply**.
9. Restart the machine for the changes to take effect.

Configure single sign-on on StoreFront

STOREFRONT CONFIGURATION

1. Launch **Citrix Studio** on the StoreFront server and select **Stores** > **Manage Authentication Methods - Store**.
2. Select **Domain pass-through**.



Domain pass-through (Single Sign-on) authentication with Kerberos

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

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

When enabled, Kerberos authenticates without passwords for Citrix Workspace app. As a result, prevents Trojan horse-style attacks on the user device that try to gain access to passwords. Users can log on using any authentication method and access published resources, for example, a biometric authenticator such as a fingerprint reader.

When you log on using a smart card to Citrix Workspace app, StoreFront, Citrix Virtual Apps and Desktops, and Citrix DaaS configured for smart card authentication- the Citrix Workspace app:

1. Captures the smart card PIN during single sign-on.
2. Uses IWA (Kerberos) to authenticate the user to StoreFront. StoreFront then provides your Citrix Workspace app with information about the available Citrix Virtual Apps and Desktops and Citrix DaaS.

> **Note:**

> Enable Kerberos to avoid an extran PIN prompt. If Kerberos authentication isn't used, Citrix Workspace app authenticates to StoreFront using the smart card credentials.

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

To use Kerberos authentication with Citrix Workspace app, check if the Kerberos configuration conforms to the following.

- Kerberos works only between Citrix Workspace app and servers that belong to the same or to trusted Windows Server domains. Servers are trusted for delegation, an option you configure through the Active Directory Users and Computers management tool.
- Kerberos must be enabled both on the domain and Citrix Virtual Apps and Desktops and Citrix DaaS. For enhanced security and to make sure that Kerberos is used, disable any non-Kerberos IWA options on the domain.
- Kerberos logon isn't available for Remote Desktop Services connections that're configured to use either Basic authentication, always use specified logon information, or always prompt for a password.

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

Domain pass-through (Single Sign-on) authentication with Kerberos for use with smart cards

Before continuing, see Secure your deployment section in the Citrix Virtual Apps and Desktops document.

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

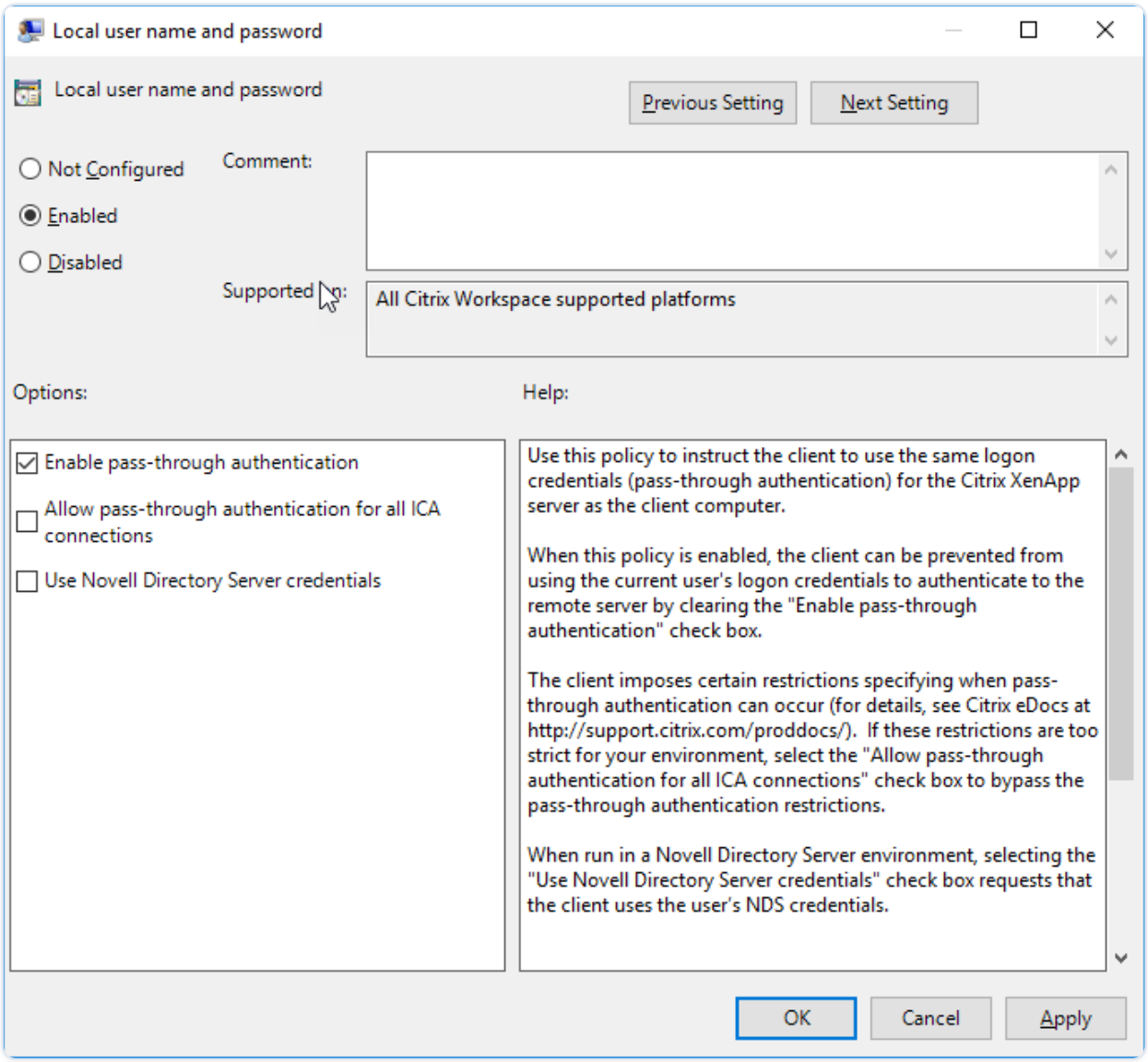
- `/includeSSON`

This option installs the single sign-on component on the domain-joined computer, enabling your workspace to authenticate to StoreFront using IWA (Kerberos). The single sign-on component stores the smart card PIN, used by the HDX engine when it remotes the smart card hardware and credentials to Citrix Virtual Apps and Desktops and Citrix DaaS. Citrix Virtual Apps and Desktops and Citrix DaaS automatically selects a certificate from the smart card and gets the PIN from the HDX engine.

A related option, `ENABLE_SSON`, is enabled by default.

If a security policy prevents you from enabling single sign-on on a device, configure Citrix Workspace app using Group Policy Object administrative template.

1. Open the Citrix Workspace app Group Policy Object administrative template by running gpedit.msc.
2. Choose **Administrative Templates** \> **Citrix Components** \> **Citrix Workspace** \> **User authentication** \> **Local user name and password**
3. Select **Enable pass-through authentication**.
4. Restart Citrix Workspace app for the changes to take effect.



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.

Enhanced domain pass-through for single sign-on

Enhanced domain pass-through for single sign-on uses Kerberos to enable single sign-on into Citrix Workspace app and into the virtual apps and desktop sessions when using Active Directory (AD) joined client devices and Citrix StoreFront.

Note:

- This feature is not supported on 32-bit operating systems.
- This feature is a replacement for the legacy pass-through authentication feature based on the Citrix Single Sign-on Service (ssonsvr.exe).
- You can't use legacy domain pass-through (SSON) authentication and enhanced domain pass-through for authentication to the same session host.
- The legacy domain pass-through (SSON) authentication requires enabling the **Enable MPR notifications for the System** policy in the Group Policy Object template. Enhanced domain pass-through, however, allows pass-through authentication without needing to enable this policy.
- For cross-domain authentication, a 2-way transitive trust is required to be able to obatin service tickets across domain boundaries. Otherwise, Kerberos delegation will not work.

Starting with Citrix Workspace™ app for Windows version 2503, the system installs SSON by default in dormant mode. You can enable SSON post-installation using the Group Policy Object (GPO) policy. To enable, navigate to **User Authentication > Local user name and password** and select the **Enable pass-through authentication** checkbox.

Note:

You must reboot the system after updating the GPO policy for the SSON setting to take effect.

System requirements

- Control plane
  - Citrix DaaS™
  - Citrix Virtual Apps and Desktops™ 2311 or later
- Virtual Delivery Agent
  - Windows: version 2308 or later

> **Note:**
>
> If either the session hosts or client devices are running **Windows 11**, VDA version **2407** or later, or **2402 LTSR CU2** or later, is required. You can download the VDA version from the Citrix downloads page.

- Citrix Workspace app: version 2309 or later

> **Note:**
>
> If either the session hosts or client devices are running **Windows 11**, Workspace app version **2405.10** or later, or **2402 LTSR CU2** or later, is required.

- Client device
  - Joined to Active Directory domain
  - Windows 10 64-bit
  - Windows 11 64-bit

> **Note:**
>
> - The client device must have direct connectivity to domain controllers. If the device is outside the network, single sign-on is not supported.

- Multi-session session hosts:
  - Windows Server 2016

    > **Note:**
    >
    > Windows Server 2016 is not supported with VDA version 2407 and later.

  - Windows Server 2019
  - Windows Server 2022

  - Windows 10 Enterprise multi-session 22H2
  - Windows 11 Enterprise multi-session 22H2 or later
- Single-session session hosts:
  - Windows 10 version 22H2
  - Windows 11 version 22H2 or later

> **Note:**
>
> Enhanced domain passthrough for single sign-on relies on Remote Credential Guard. Make sure to review the Remote Credential Guard requirements and supported authentication scenarios in the Microsoft documentation.

Known issues

- When Windows Defender Credential Guard is enabled on the client device, single sign-on into the session will fail and a Windows Security prompt will appear stating `Your credentials did not work. Windows Defender Credential Guard does not allow using Windows logon credentials. Please enter your credentials.` Upgrade to Citrix Workspace app for Windows 2507 CU3, 2607 LTSR, or later to resolve the issue.

  Alternatively, as a workaround, you can disable Windows Defender Credential Guard. Following are two options to disable the feature:

  a. Using Group Policy, configure the setting **Turn On Virtualization Based Security** under **Computer Configuration** > **Administrative Templates** > **System** > **Device Guard**.

  b. In the registry, under `HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Lsa`, set the `LsaCfgFlags` value to `0`.

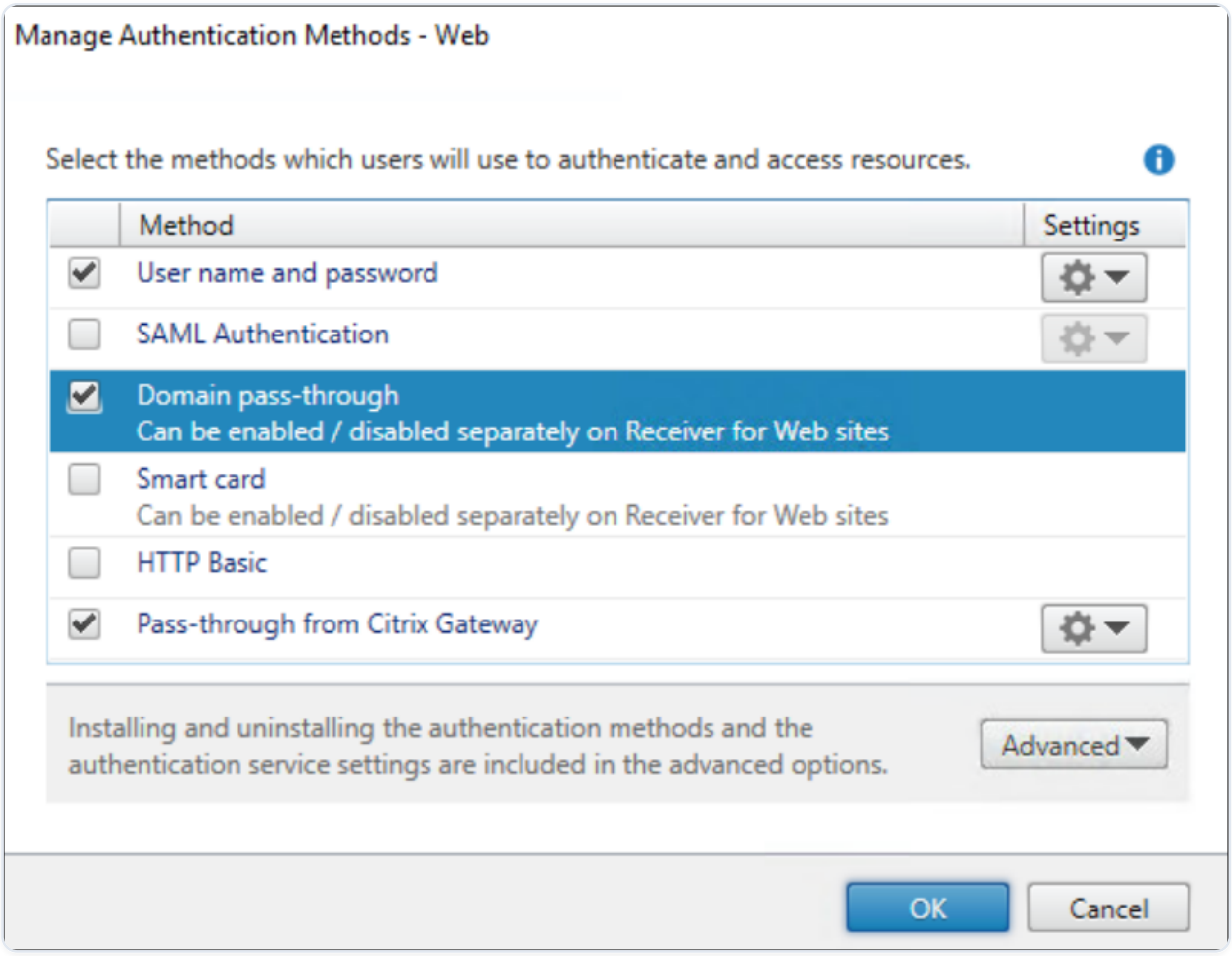
StoreFront™ configuration

You must enable domain pass-through authentication for the store and its corresponding website.

Perform the following steps to enable Domain pass-through for the store:

1. Open the StoreFront management console.
2. Go to **Store** > **Manage Authentication methods**. The **Manage Authentication Methods - Web** window appears.

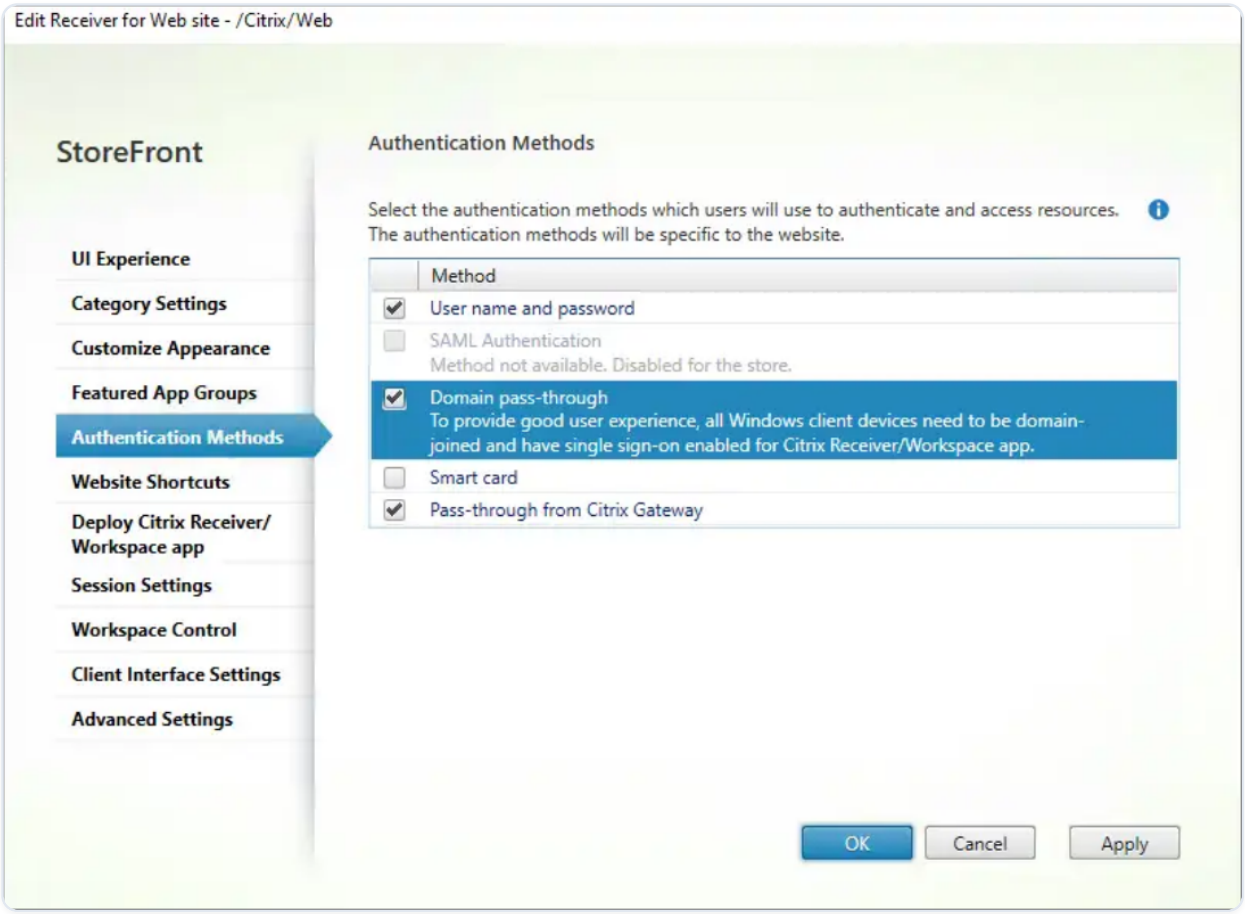
3. Select the **Domain pass-through** checkbox.



4. Click **OK**.

Perform the following steps to enable Domain pass-through for the website:

1. Open the StoreFront management console.
2. Open **Stores** > **Receiver for Websites** tab > **Manage Receiver for Web Sites** > **Configure** > **Authentication Methods**. The **Edit Receiver for Web site - /Citrix/Web window** appears.
3. Select the **Domain pass-through** checkbox.



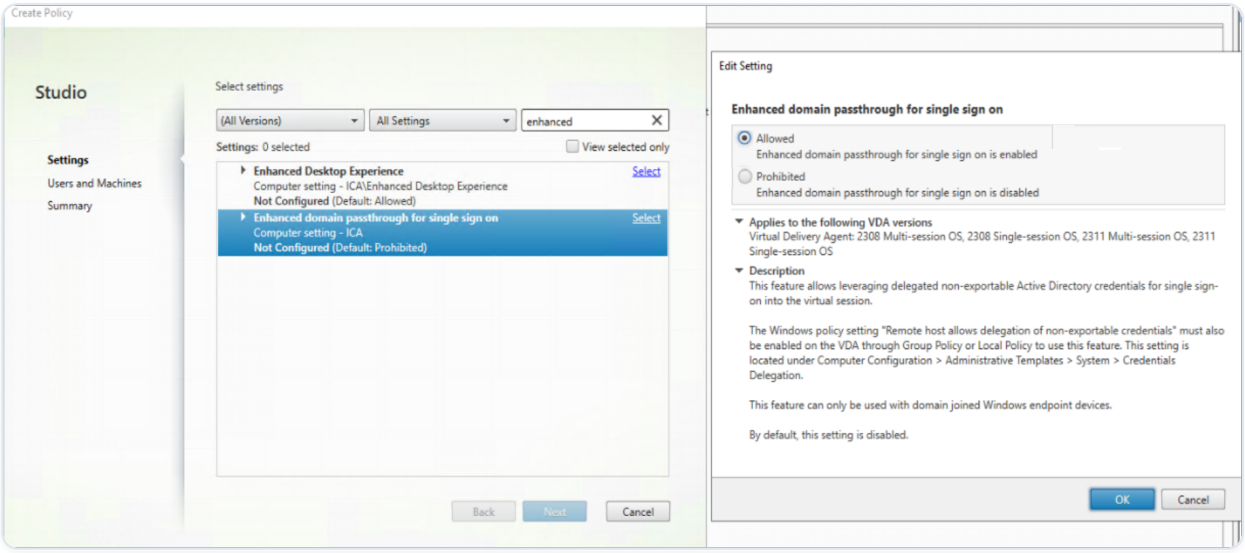
4. Click **OK**.

Citrix Policy configuration

You must enable the setting using Citrix policy:

1. Navigate to Citrix Studio or the web console.
2. Click **Policies** > **Create Policy**. The **Create Policy** dialog box appears.
3. Search for the **Enhanced domain pass-through for single sign-on** policy. The **Edit Settings** dialog box appears.

4. Select the **Allowed** option to enable the **Enhanced domain pass-through for single sign-on** policy.

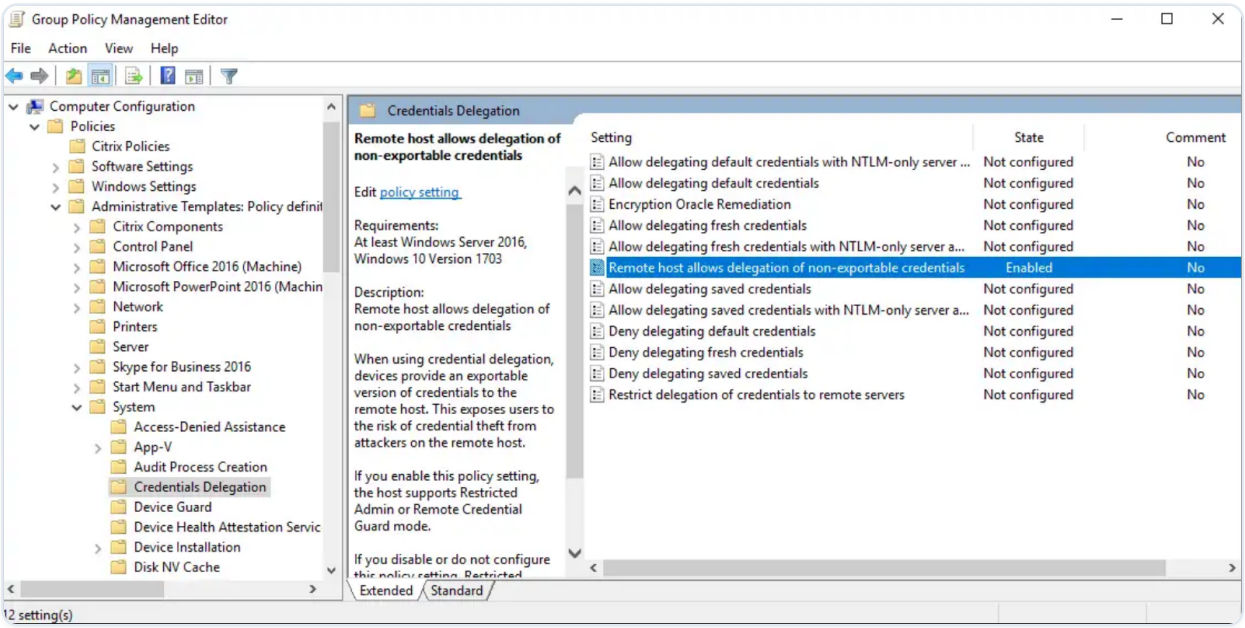


5. Click **OK**.

Session host configuration

After enabling the **Enhanced domain pass-through for single sign on** feature using Citrix policy, you must also enable a Windows setting on the session hosts. You can enable the Windows setting through local policy or GPO:

1. Navigate to `Computer Configuration\Policies\Administrative Templates\System\CredentialsDelegation`.
2. Enable the **Remote host allows delegation of non-exportable credentials** setting.



3. Reboot the session host for the setting to take effect.

Note:

The **Remote host allows delegation of non-exportable credentials** setting is not available on Windows Server 2016 local policy. If you need to configure this setting locally on the session host instead of using GPO, you must add the following registry value:

Key: HKLM\SYSTEM\CurrentControlSet\Control\Lsa

- Value type: DWORD
- Value name: DisableRestrictedAdmin
- Value data: 0

Client device configuration

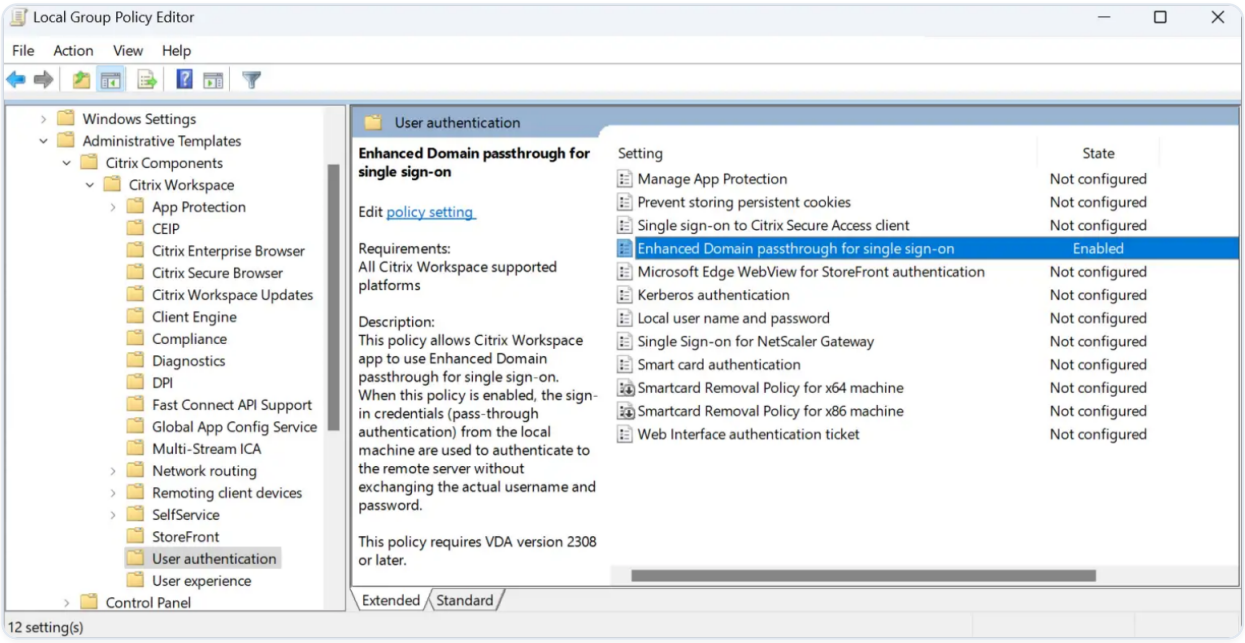
You must do the following on client device:

- Enable Enhanced domain pass-through for single sign-on
- Trust StoreFront site

Enable Enhanced domain pass-through for single sign-on

You must enable the **Enhanced domain pass-through for single sign on feature** on the client device. You can do this through local policy or GPO.

1. Navigate to `Computer Configuration\Policies\Administrative Templates\Citrix Components\Citrix Workspace\User Authentication`.
2. Enable the **Enhanced Domain pass-through for single sign-on** setting.

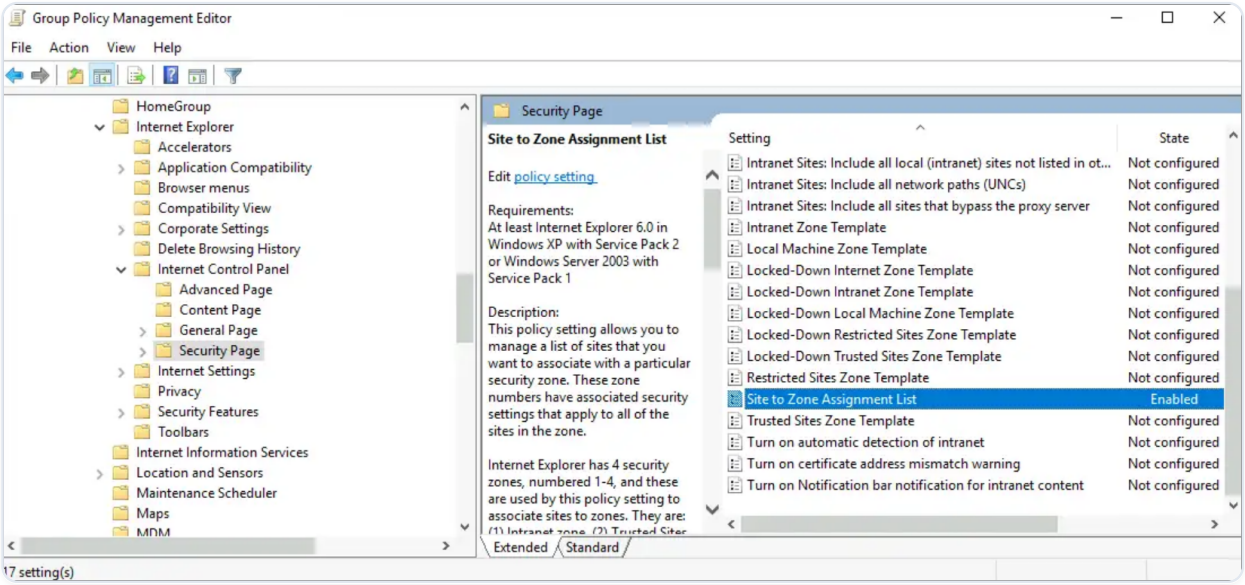


3. Restart Citrix Workspace app for settings to take effect.

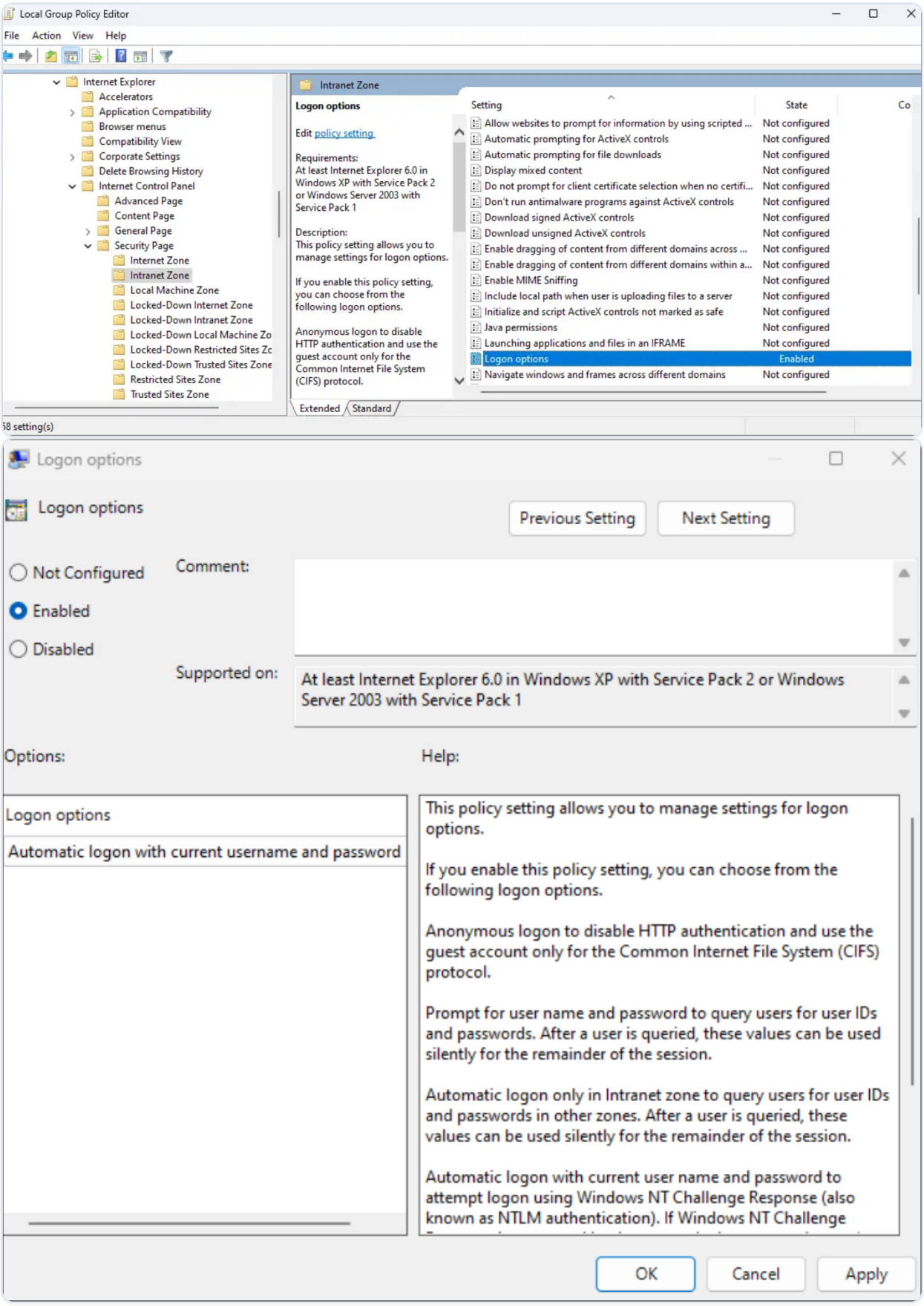
Trust StoreFront site

You must make sure your StoreFront URL is trusted by the client devices. If the URL is not part of an already trusted domain, you must add it as either a local intranet site or a trusted site. You can do this through local policy or GPO.

1. Navigate to `Computer Configuration\Policies\Administrative Templates\Windows Components\Internet Explorer\Internet Control Panel\Security` page.
2. Enable the **Site to Zone Assignment List** setting and add the appropriate URLs and corresponding zone assignment.



3. Enable the **Logon options** setting and set it to **Automatic logon** with current username and password.


Local Group Policy Editor
File Action View Help
Internet Explorer
Accelerators
Application Compatibility
Browser menus
Compatibility View
Corporate Settings
Delete Browsing History
Internet Control Panel
Advanced Page
Content Page
General Page
Security Page
Internet Zone
Intranet Zone
Local Machine Zone
Locked-Down Internet Zone
Locked-Down Intranet Zone
Locked-Down Local Machine Zo
Locked-Down Restricted Sites Zc
Locked-Down Trusted Sites Zone
Restricted Sites Zone
Trusted Sites Zone
Intranet Zone
Logon options
Edit policy setting
Requirements:
At least Internet Explorer 6.0 in Windows XP with Service Pack 2 or Windows Server 2003 with Service Pack 1
Description:
This policy setting allows you to manage settings for logon options.
If you enable this policy setting, you can choose from the following logon options.
Anonymous logon to disable HTTP authentication and use the guest account only for the Common Internet File System (CIFS) protocol.
Setting
State
Allow websites to prompt for information by using scripted ... Not configured
Automatic prompting for ActiveX controls Not configured
Automatic prompting for file downloads Not configured
Display mixed content Not configured
Do not prompt for client certificate selection when no certifi... Not configured
Don't run antimalware programs against ActiveX controls Not configured
Download signed ActiveX controls Not configured
Download unsigned ActiveX controls Not configured
Enable dragging of content from different domains across ... Not configured
Enable dragging of content from different domains within a... Not configured
Enable MIME Sniffing Not configured
Include local path when user is uploading files to a server Not configured
Initialize and script ActiveX controls not marked as safe Not configured
Java permissions Not configured
Launching applications and files in an IFRAME Not configured
Logon options Enabled
Navigate windows and frames across different domains Not configured
Extended Standard
58 setting(s)
Logon options
Logon options
Previous Setting
Next Setting
Not Configured
Enabled
Disabled
Comment:
Supported on:
At least Internet Explorer 6.0 in Windows XP with Service Pack 2 or Windows Server 2003 with Service Pack 1
Options:
Help:
Logon options
Automatic logon with current username and password
This policy setting allows you to manage settings for logon options.
If you enable this policy setting, you can choose from the following logon options.
Anonymous logon to disable HTTP authentication and use the guest account only for the Common Internet File System (CIFS) protocol.
Prompt for user name and password to query users for user IDs and passwords. After a user is queried, these values can be used silently for the remainder of the session.
Automatic logon only in Intranet zone to query users for user IDs and passwords in other zones. After a user is queried, these values can be used silently for the remainder of the session.
Automatic logon with current user name and password to attempt logon using Windows NT Challenge Response (also known as NTLM authentication). If Windows NT Challenge
OK
Cancel
Apply

Configuring single sign-on to Citrix Workspace app

Single sign-on using Azure Active Directory

This section explains how to implement single sign-on (SSO) using Azure Active Directory (AAD) as an identity provider with domain joined workloads in hybrid or AAD enrolled endpoints. With this configuration, you can authenticate to Workspace using Windows Hello or FIDO2 on endpoints that are enrolled to AAD.

> **Note:**
>
> If you use Windows Hello, as a standalone authentication, you can achieve single sign-on to Citrix Workspace app. However, you are prompted for your user name and password while accessing published virtual apps or desktops. As a workaround, consider implementing Federated Authentication Service (FAS).

Prerequisites

- An active Azure Active Directory connection to Citrix Cloud. For more information, see Connect Azure Active Directory to Citrix Cloud.
- An Azure Active Directory workspace authentication. For more information, see Enable Azure AD authentication for workspaces.
- Verify if you have configured Azure AD Connect. For more information, see Getting started with Azure AD Connect using express settings.
- Activate Pass-through authentication on Azure AD Connect. Also, verify if the single sign-on and the Pass-through options work on the Azure portal. For more information, see Azure Active Directory Pass-through Authentication: Quickstart.

Configuration

Do the following steps to configure SSO on your device:

1. Install the Citrix Workspace app using the Windows command line with the `includeSSON` option:

```
CitrixWorkspaceApp.exe /includeSSON
```

1. Reboot your device.

Starting with Citrix Workspace™ app for Windows version 2503, the system installs SSON by default in dormant mode. You can enable SSON post-installation using the Group Policy Object (GPO) policy. To enable, navigate to **User Authentication > Local user name and password** and select the **Enable pass-through authentication** checkbox.

> **Note:**
>
> You must reboot the system after updating the GPO policy for the SSON setting to take effect.

2. Open the Citrix Workspace app Group Policy Object administrative template by running `gpedit.msc`.
3. Go to **Administrative Templates** > **Citrix Components** > **Citrix Workspace** > **User Authentication** > **Local user name and password**.
4. Select **Enable pass-through authentication**. Depending on the configuration and security settings, select the **Allow pass-through authentication for all ICA®** option for pass-through authentication to work.
5. Modify the User Authentication settings in Internet Explorer. To modify the settings:
    - Open **Internet Properties** from the Control panel.
    - Navigate to **General Properties** > **Local Intranet** and click **Sites**.
    - In the **Local Intranet** window, click **Advanced, add trusted sites**, add the following trusted sites, and click **Close**:
        - `https://aadg.windows.net.nsatc.net`
        - `https://autologon.microsoftazuread-sso.com`
        - `The name of your tenant, for example: https://xxxtenantxxx.cloud.com`
6. Disable extra authentication prompts by disabling Always prompt end users for their credentials.
7. Enable domain pass-through authentication on the Citrix Workspace app client. For more information, see Domain pass-through authentication.
8. Restart the Citrix Workspace app for the changes to take effect.

Single sign-on using Okta and Federated Authentication Service

This section explains how you can implement single sign-on (SSO) using Okta as an identity provider with domain joined device and Federated Authentication Service (FAS). With this configuration, you can authenticate to Workspace using Okta to enable single sign-on and prevent a second logon prompt. For this authentication mechanism to work, you need to use the Citrix Federated Authentication Service with Citrix Cloud. For more information, see Connect Citrix Federated Authentication Service to Citrix Cloud.

Prerequisites

- Cloud Connector. For more information about installing the Cloud Connector, see Cloud Connector Installation.
- An Okta agent. For more information about installing an Okta agent, see Install the Okta Active Directory agent. Also, you can cofigure the Okta IWA Web agent to login from a Windows Domain joined device. For more information, see Install and configure the Okta IWA Web agent for Desktop single sign-on
- An active Azure Active Directory connection to Citrix Cloud. For more information, see Connect Azure Active Directory to Citrix Cloud.
- Federated Authentication Service. For more information, see Install the Federated Authentication Service.

Configuration

Do the following steps to configure SSO on your device:

Connect Citrix Cloud™ to your Okta organization:

1. Download and install the Okta Active Directory agent. For more information, see Install the Okta Active Directory agent.
2. Sign in to Citrix Cloud at `https://citrix.cloud.com`.
3. From the Citrix Cloud menu, select **Identity and Access Management**.
4. Locate Okta and select **Connect** from the ellipsis menu.
5. In **Okta URL**, enter your Okta domain.
6. In **Okta API Token**, enter the API token for your Okta organization.
7. In **Client ID** and **Client Secret**, enter the client ID and secret from the OIDC web app integration you created earlier. To copy these values from the Okta console, select **Applications** and locate your Okta application. Under **Client Credentials**, use the **Copy to Clipboard** button for each value.

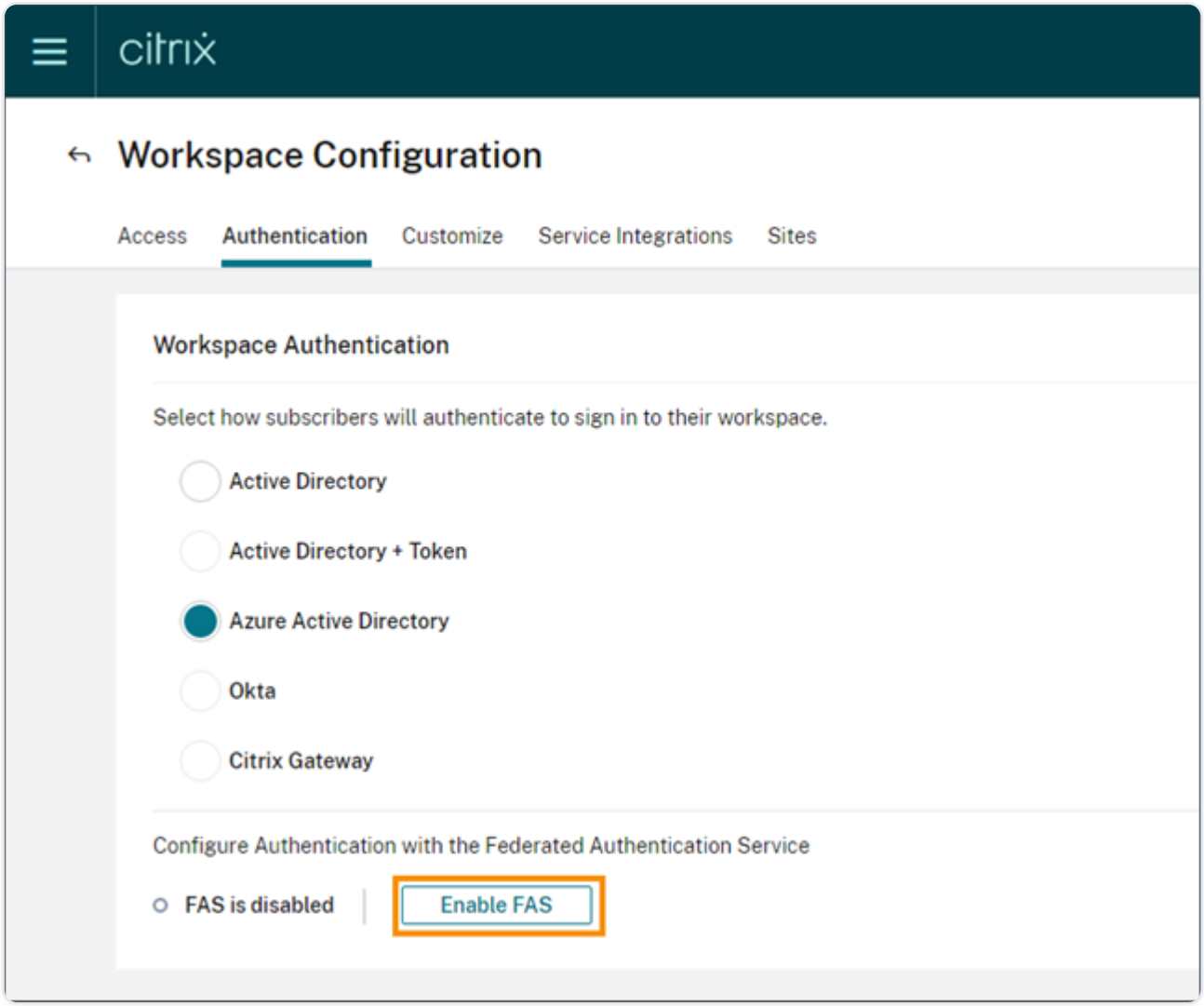
8. Click **Test and Finish**. Citrix Cloud verifies your Okta details and tests the connection.

Enable Okta authentication for workspaces:

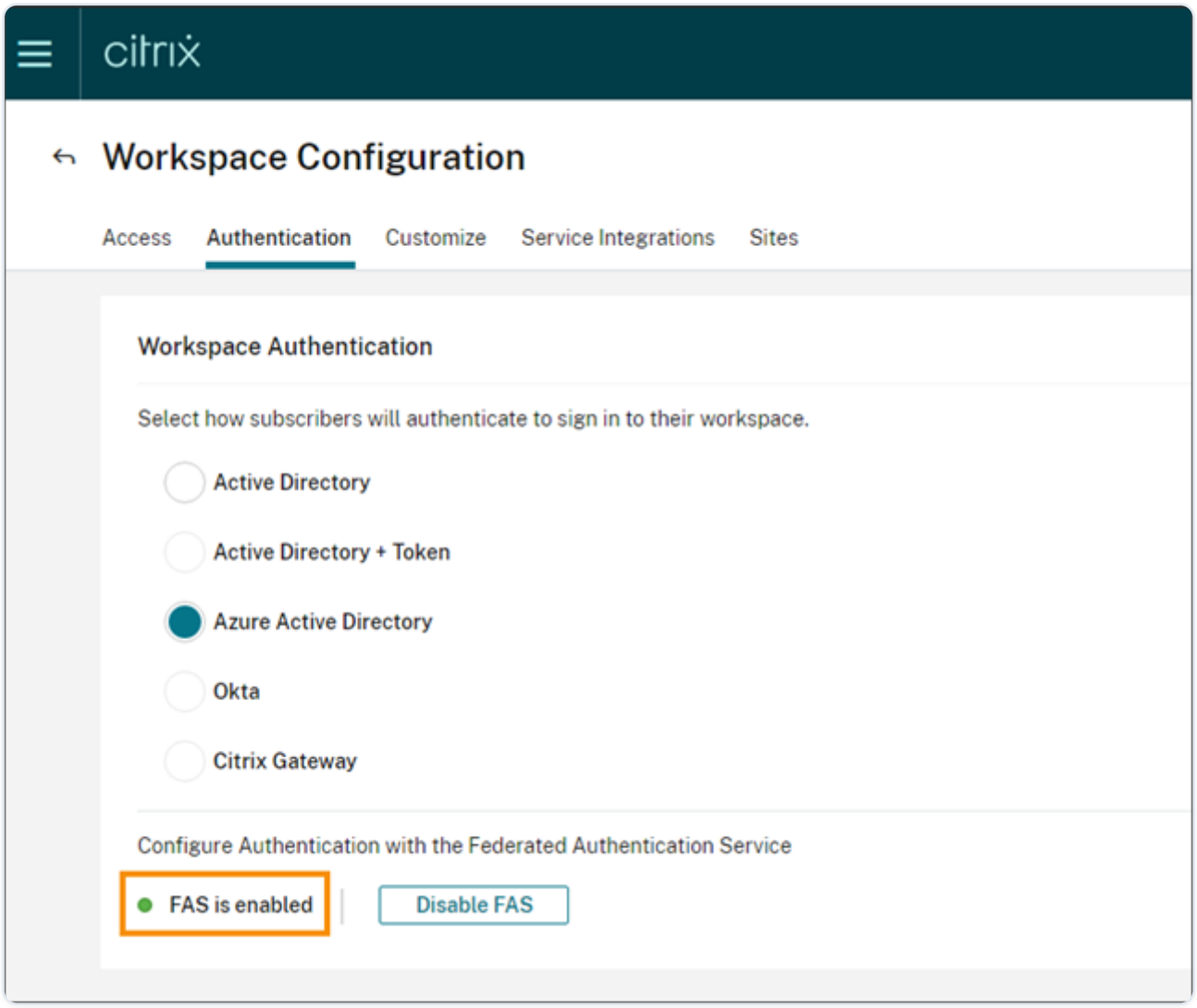
1. From the Citrix Cloud menu, select **StoreFront Cloud** > **Authentication**.
2. Select **Okta**. When prompted, select **I understand the impact on the subscriber experience**.
3. Click **Accept** to accept the permissions request.

Enable Federated Authentication Service:

1. From the Citrix Cloud menu, select **StoreFront Cloud** and then select **Authentication**.
2. Click **Enable FAS**. This change might take up to five minutes to be applied to subscriber sessions.



Afterward, the Federated Authentication Service is active for all virtual app and desktop launches from Citrix Workspace.



When subscribers sign in to their workspace and launch a virtual app or desktop in the same resource location as the FAS server, the app or desktop starts without prompting for credentials.

Note:

If all FAS servers in a resource location are down or in maintenance mode, application launches succeed, but single sign-on isn't active. Subscribers are prompted for their AD credentials to access each application or desktop.

HDX™

This section describes the following:

- Graphics and display
- Optimized Microsoft Teams
- HDX transport
- Browser content redirection
- Bidirectional content redirection
- ICA settings reference

Graphics and display

Multi-monitor support

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

Each monitor in a multiple monitor configuration has its own resolution designed by its manufacturer. Monitors can have different resolutions and orientations during sessions.

Sessions can span multiple monitors in two ways:

- Full screen mode, with multiple monitors shown inside the session; applications snap to monitors as they would locally.

  Citrix Virtual Apps and Desktops™ and Citrix DaaS: To display the Desktop Viewer window across any rectangular subset of monitors, resize the window across any part of those monitors and click **Maximize**.
- Windowed mode, with one single monitor image for the session, applications do not snap to individual monitors.

Citrix Virtual Apps and Desktops and Citrix DaaS: When any desktop in the same assignment (formerly "desktop group") is launched then, the window setting is preserved and the desktop is displayed across the same monitors. Multiple virtual desktops can be displayed on one device provided the monitor arrangement is rectangular. If the primary monitor on the device is used by

the virtual apps and desktops session, it becomes the primary monitor in the session. Otherwise, the numerically lowest monitor in the session becomes the primary monitor.

To enable multi-monitor support, check the following:

- The user device is configured to support multiple monitors.
- The operating system can detect each of the monitors. On Windows platforms, to verify that this detection occurs, go to **Settings** > **System** and click **Display** and confirm that each monitor appears separately.
- After your monitors are detected, ensure the **Display memory limit** policy is set on VDA:
    - **Citrix Virtual Desktops™:** Configure the graphics memory limit using the **Citrix Machine Policy** setting Display memory limit.
    - **Citrix Virtual Apps:** Depending on the version of the Citrix Virtual Apps server, you've installed configure the graphics memory limit using the **Citrix Computer Policy** setting Display memory limit.

  For more information, see Display memory limit documentation.

Check if the setting is large enough (in kilobytes) to provide sufficient graphic memory. If this setting isn't high enough, the published resource is restricted to the subset of the monitors that fits within the size specified.

Using Citrix Virtual desktops on dual monitor:

1. Select the Desktop Viewer and click the down arrow.
2. Select **Window**.
3. Drag the Citrix Virtual Desktops screen between the two monitors. Ensure that about half the screen is present in each monitor.
4. From the Citrix Virtual Desktop toolbar, select **Full-screen**.

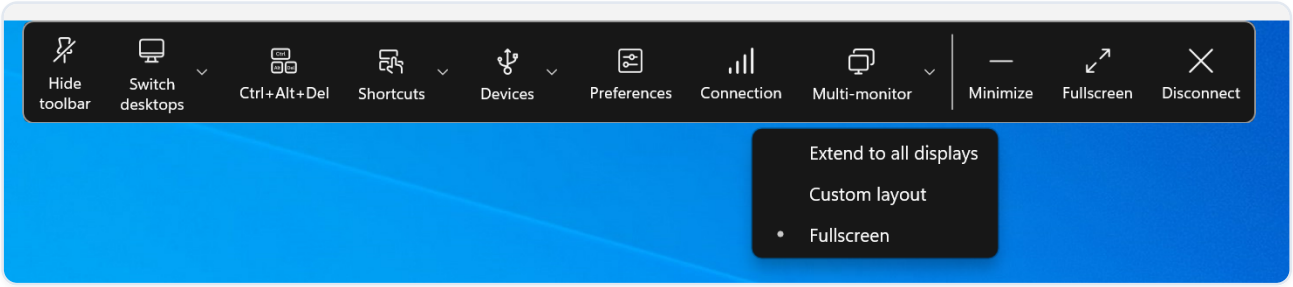
   The screen is now extended to both the monitors.

For calculating the session's graphic memory requirements for Citrix Virtual Apps and Desktops and Citrix DaaS, see Knowledge Center article CTX115637.

Multi-monitor layout selection

Starting with version 2503, the **Multi-Monitor Selector (MMS)** allows users to choose which displays to use in full-screen mode for desktop sessions only, not for seamless sessions. A new **Multi-Monitor** button has been added to the toolbar, which appears only when more than one

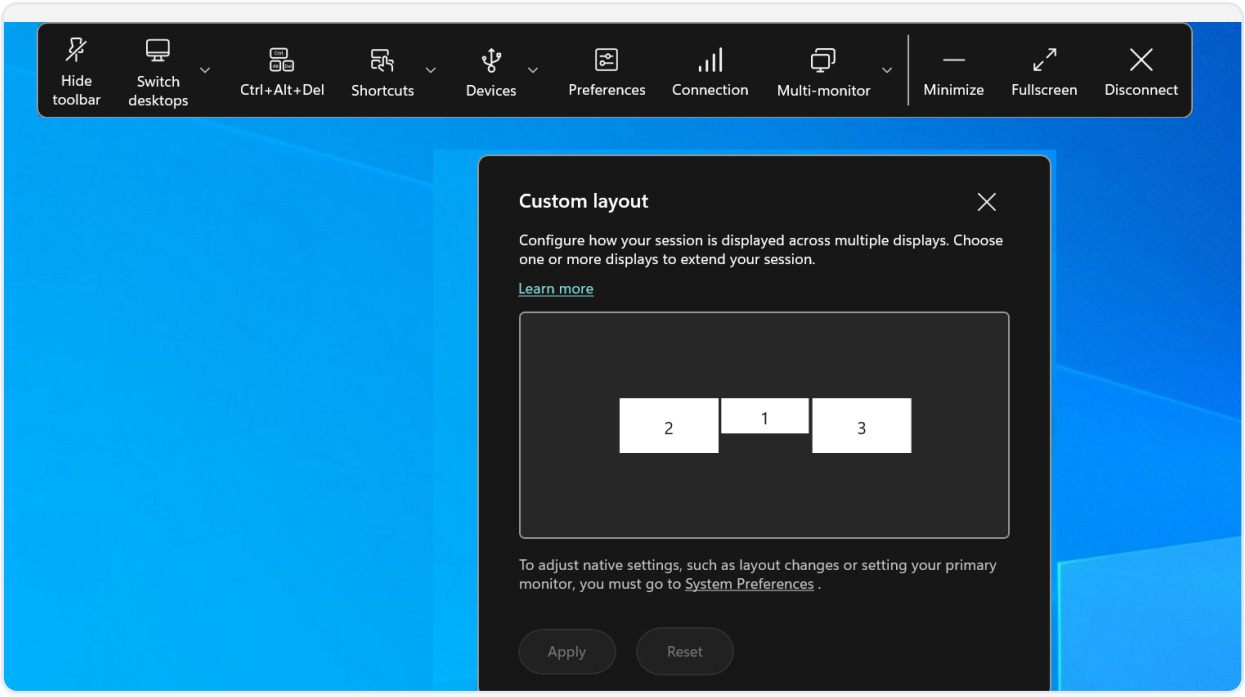
screen is connected. This feature enhances the flexibility and usability of multi-monitor setups in desktop sessions, providing a more tailored and efficient user experience.



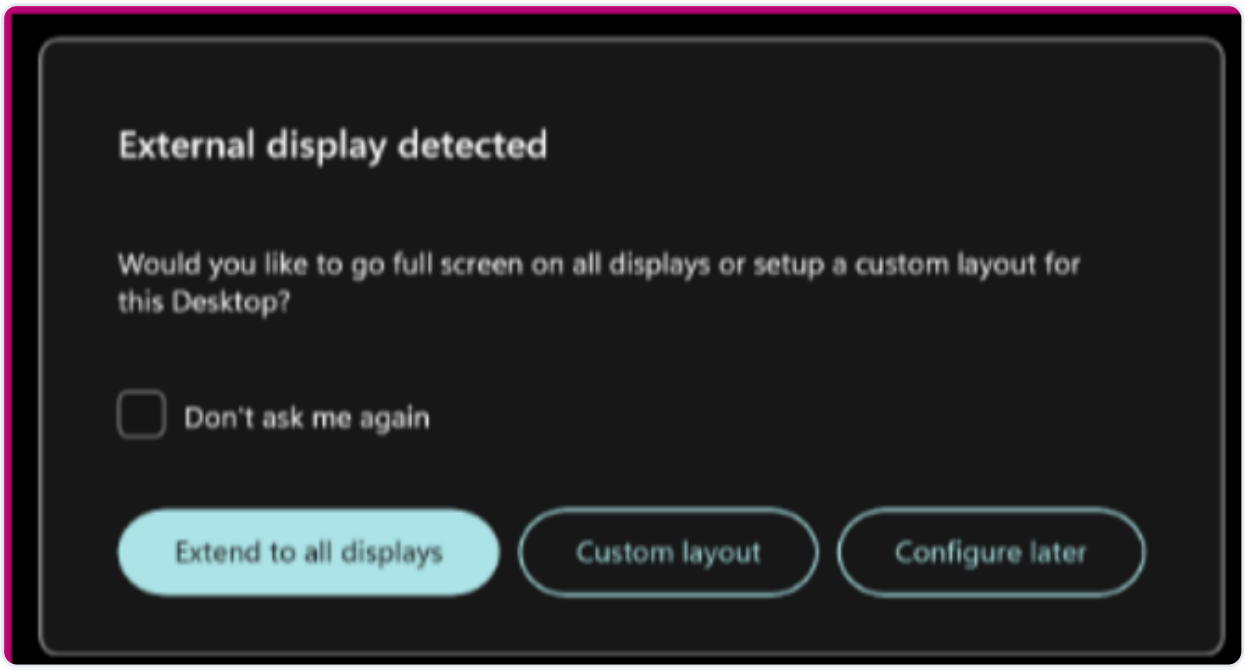
Multi-monitor menu options

The toolbar button includes three drop-down menu options for desktop sessions in full-screen mode:

- **Extend to All Displays**: The session switches to full-screen mode on all connected screens.
- **Custom Layout**: This option opens a custom monitor selector displaying the layout of the Windows system. Users can click the rectangles in the selector to choose which screens to use and then click **Apply**. The session then uses the selected screens in full-screen mode.



- **Fullscreen**: The session switches to full-screen mode on whichever monitor the session is currently active on. For example:
  - If your session is active on one monitor, it will be full screen on that monitor.
  - If your session is active on two monitors, it will be full screen on those two monitors.



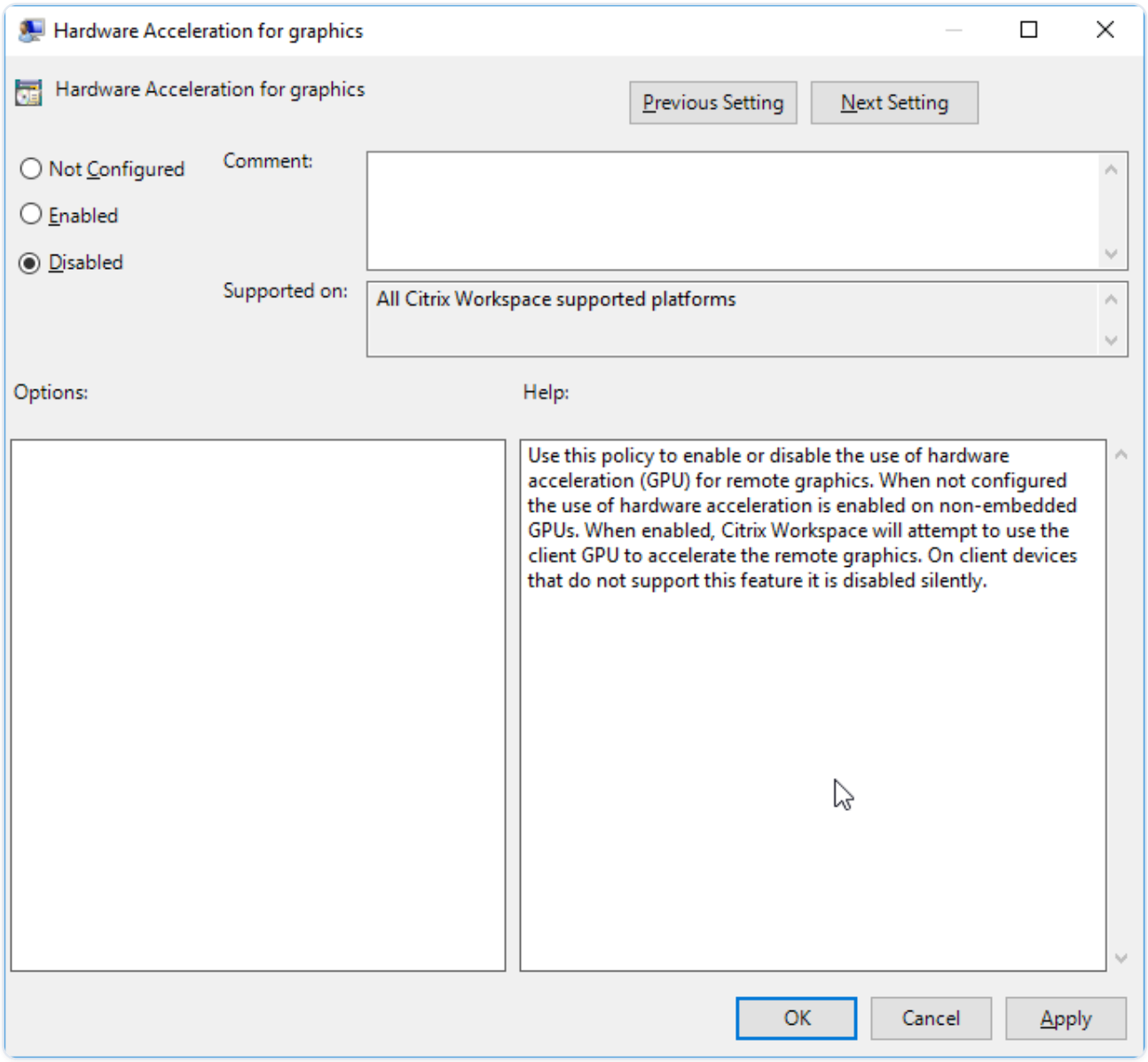
When a new monitor is plugged in, a notification appears for the user to make a selection. Users can check **Remember my preference** to mute this notification.

Hardware decoding

When using Citrix Workspace app (with HDX engine), the GPU can be used for video decoding wherever it's available at the client. This feature is enabled by default.

To disble 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 **Disabled** and click **Apply** and **OK**.



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

- If the client has two GPUs and if one of the monitors is active on the second GPU, CPU decoding is used.
- When connecting to a Citrix Virtual Apps server running on Windows Server 2008 R2, don't use hardware decoding on the user's Windows device. If enabled, issues like slow performance while highlighting text and flickering issues are seen.

Virtual display layout

This feature lets you define a virtual monitor layout that applies to the remote desktop. You can also split a single client monitor virtually into up to eight monitors on the remote desktop. You can configure the virtual monitors 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.

Starting from Citrix Workspace app for Windows 2106, virtual display layout is also supported for full-screen and multi-monitor desktop sessions. Virtual display layout is enabled by default. In a multi-monitor scenario, the same virtual display layout is applied to all the session monitors if the total number of virtual displays doesn't exceed eight virtual displays. In case this limit is exceeded, the virtual display layout is ignored and not applied to any session monitor.

Multi-monitor enhancement can be disabled by setting the following registry key:

- `HKEY_CURRENT_USER\Software\Citrix\XenDesktop\DesktopViewer`

Name: **SplitAllMonitors** Type: DWORD

Values:

1 - Enabled

0 - Disabled

DPI scaling

Citrix Workspace app is DPI aware and supports matching display resolution and DPI scale settings on the Windows client to the virtual apps and desktops session.

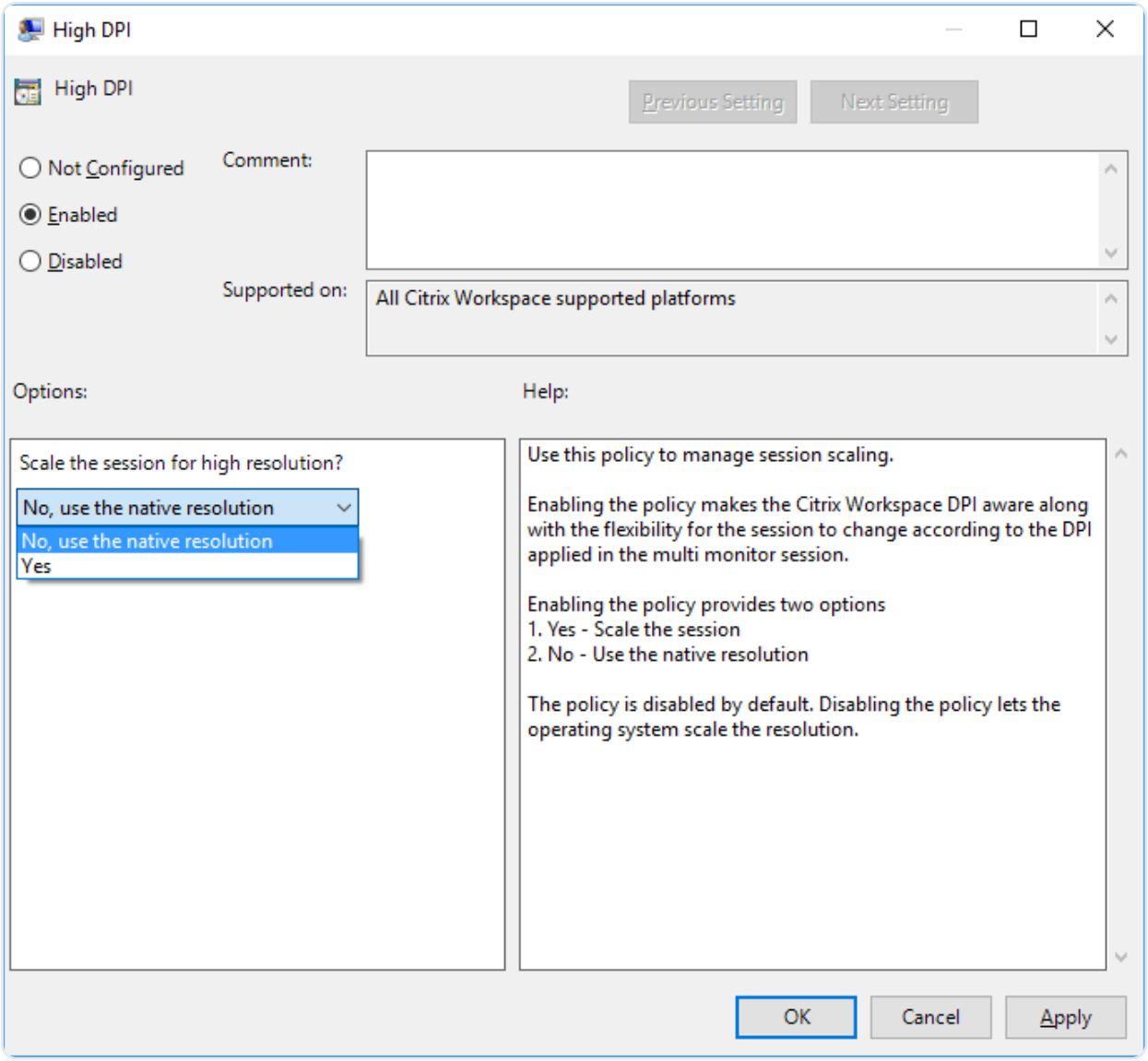
DPI scaling is mostly used with large size and high-resolution monitors to display applications, text, images, and other graphical elements in a size that can be viewed comfortably.

This feature is enabled by default, and it is the recommended setting for all use cases. However, administrators can still configure the DPI scaling using Group Policy Object (GPO) administrative template (per-machine configuration) if necessary.

To configure DPI scaling using GPO administrative template:

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 the client scale up the session locally.
   b. No, use the native resolution - Indicates that the Citrix Workspace app detects the DPI on the client and the client applies it to the VDA.
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:

1. Right-click Citrix Workspace app icon from the notification area.
2. Select **Advanced Preferences** and click **High DPI** setting.
3. Select one of the following options:
    a. **Yes** - Indicates that the client scale up the session locally.
    b. **No, use the native resolution** - Indicates that the Citrix Workspace app detects the DPI on the client and the client applies it to the VDA. By default, this option is selected.
    c. **Let the operating system scale the resolution** - 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.

NOTE:

> **Additional considerations:**

> - DPI matching requires Citrix Virtual Apps and Desktops versions 1912 LTSR or later.
> - The **No, use the native resolution** (DPI matching) setting is recommended in most cases.
> - The **Let the operating system scale the resolution** setting disables DPI awareness on the Citrix Workspace App. This mode might result in blurry graphics when the Windows client DPI scale is set to anything other than 100%. This mode doesn't support multiple monitors with different DPI scales.
> - The **Yes** option results in the Citrix Workspace app upscaling the session window to match the DPI scale configured on the Windows client. This is a legacy function recommended only for connections to legacy XenApp and XenDesktop environments when DPI scales above 100% are required on the client. This mode might result in blurry graphics.

> For information about troubleshooting issues with DPI scaling, see Knowledge Center article CTX230017.

Enabling DPI matching

Starting with Citrix Workspace app 2206 for Windows, DPI matching is enabled by default. This means Citrix Workspace app attempts to match display resolution and DPI scale settings of the local Windows client to the Citrix session automatically. As part of this change, the High DPI option available under Advance Preferences in Citrix Workspace app is no longer available.

Automatic selection of video codec

Starting with 2311.1 release, Citrix Workspace app for Windows now automatically detects the best video codec to use. During installation of the Citrix Workspace app for Windows, the decoding capabilities of the endpoint are evaluated. Based on this information, Citrix Workspace app for Windows selects the best codec to use with the VDA when the session starts. The order in which the video codecs are evaluated is as follows:

1. AV1
2. H.265
3. H.264

This feature is available when the **Use video codec for compression** policy is set to one of the following:

- **Use when preferred**
- **For the entire screen**
- **For actively changing regions**

For more information on the **Use video codec for compression** policy, see Use video codec for compression.

The automatic selection only applies to YUV 4:2:0 variants of these codecs. YUV 4:2:0 uses less bandwidth compromising quality. If the **Visual Quality** policy setting is set to **Build-to-Lossless** or **Always Lossless** and if the **Allow Visually Lossless** policy is set to **enabled**, the automatic selection of the video codec is disabled and instead YUV 4:4:4 H.264 or H.265 is used.

For more information on these policies, see the following:

- Visual Quality
- Allow visually lossless compression

> **Note:**

> YUV 4:2:0 is a chroma subsampling and is a color compression technique which lowers overall bandwidth consumption.

> When connecting to a resource, Citrix Workspace app tests the endpoint's capability to decode H.265 and AV1 and save the capabilities in the registry. After that Citrix Workspace app automatically selects the best video codec to use and negotiates this codec with the VDA. If both the VDA and the client can use H.265 and AV1, AV1 is selected as the video codec. If AV1 is not available on either the VDA or on the client, H.265 is selected. If H.265 is also not available on either, the session uses H.264 as the video codec.

This feature is enabled by default.

To disable the automatic selection of the video codec, set **DisableDecoderCaps** as follows:

1. Open the Registry Editor using `regedit` on the Run command.
2. Navigate to `HKEY_LOCAL_MACHINE\Software\WOW6432Node\Policies\Citrix\ICA Client\Graphics Engine`.

   Or,

   Navigate to `HKEY_CURRENT_USER\Software\Policies\Citrix\ICA Client\Graphics Engine`
3. Create a DWORD key by the name **DisableDecoderCaps** and set the value of the key to 1.

If the value of **DisableDecoderCaps** is set to 1 in HKEY_LOCAL_MACHINE or HKEY_CURRENT_USER, the automatic selection of the video codec isn't used.

H.265 video encoding

Citrix Workspace app supports the use of the H.265 video codec for hardware acceleration of remote graphics and videos. H.265 video codec must be supported and enabled on both the VDA and Citrix Workspace app.

Prerequisites:

- VDA 2203 and later.
- Citrix Workspace™ app for Windows 2305 or later.
- Enable the **Use hardware encoding for video codec** policy on the VDA (as per default).
- Citrix Workspace app for Windows has the following client hardware requirements for H.265:

- NVIDIA Pascal generation GPUs or later
- Intel 6th generation GPU or later
- AMD Generation GCN3 or later

Note:

This feature has more VDA requirements such as the following:

- NVIDIA Maxwell generation GPU or later
- Intel 6th generation GPU or later
- AMD Raven generation GPU or later

Starting with Citrix Workspace app 2311.1, this feature is enabled automatically with the introduction of the **Automatic selection of video codec** feature.

This behavior can be changed by explicitly controlling H.265 decoding with the client-side registry key **EnableH265**.

Configuring H.265 video encoding using the Registry editor:

Enabling H.265 video encoding on a non-domain joined network on a 32-bit operating system:

1. Open 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 the 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. Open the Registry Editor using `regedit` on the Run command.
2. Navigate to `HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Policies\Citrix\ICA Client\Graphics Engine`.
3. Create a DWORD key by the name **EnableH265** and set the value of the key to 1.
4. Restart the session for the changes to take effect.

The presence of the **EnableH265** disables auto-detection. Setting the **EnableH265** to 0 disables H.265 decoding. Therefore, the session doesn't use the H.265 video codec, even if it is configured on the VDA.

With setting **EnableH265** to 1, Citrix Workspace app for Windows tries to use H.265 decoding. If H.265 decoding fails, the client and server fall back to H.264 encoding.

Note:

- If the Hardware acceleration for Graphics policy is disabled in the Citrix Workspace app Group Policy Object administrative template, the H.265 Decoding for graphics policy settings is ignored. The feature is then not applied and falls back to using the H.264 video codec.
- The Graphics Status indicator and Citrix HDX™ monitor can be used to validate the video codec usage.

AV1

Citrix Workspace app supports the use of the AV1 video codec for hardware acceleration of remote graphics and videos. AV1 video codec must be supported and enabled on both the VDA and Citrix Workspace app.

Prerequisites for AV1 are as follows:

- VDA 2308 or later.
- Citrix Workspace app for Windows 2305 or later
- Enable the **Use hardware encoding for video codec** policy on the VDA (as per default).
- Citrix Workspace app for Windows has the following client hardware requirements for AV1:
  - NVIDIA Ampere or later
  - Intel 11th Gen / Arc or newer
  - AMD Radeon RX 6000 / Radeon Pro W6000 series (RDNA2) or later

Note:

AV1 has more VDA requirements, such as the following:

- NVIDIA Lovelace generation GPU or later (for example L4 / L40)
- Intel Arc generation GPU or later

Starting with Citrix Workspace app 2311.1, this feature is enabled automatically with the introduction of the **Automatic selection of video codec** feature.

This behavior can be changed by explicitly controlling AV1 decoding with the client-side registry key **EnableAV1**.

Configuring AV1 video encoding using the Registry editor:

Enabling AV1 video encoding on a non-domain joined network on a 32-bit operating system:

1. Open 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 the name **EnableAV1** and set the value of the key to 1.
4. Restart the session for the changes to take effect.

Enabling AV1 video encoding on a non-domain joined network on a 64-bit operating system:

1. Open the Registry Editor using `regedit` on the run command.
2. Navigate to `HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Policies\Citrix\ICA Client\Graphics Engine`.
3. Create a DWORD key by the name **EnableAV1** and set the value of the key to 1.
4. Restart the session for the changes to take effect.

The presence of the **EnableAV1** disables auto-detection. Setting **EnableAV1** to 0 disables AV1 decoding and therefore, the session doesn't use the AV1 video codec.

With setting **EnableAV1** to 1, Citrix Workspace app for Windows tries to use AV1 decoding. If AV1 decoding fails, the client and server fall back to H.264 encoding.

Note:

If the Hardware acceleration for Graphics policy is disabled in the Citrix Workspace app Group Policy Object administrative template, the AV1 Decoding for graphics policy settings is ignored. The feature is then not applied and falls back to using the H.264 video codec.

The Graphics Status indicator and Citrix HDX monitor can be used to validate the video codec usage.

Improved graphics performance

Citrix Workspace app 2206 introduces significant performance improvements for Intel integrated GPUs:

- Graphics GPU consumption has been reduced, improving overall performance.

The following issues are fixed:

- Low frames per second after playing a video on the Intel 10th Generation GPU or higher.
- Brightness difference in Build-To-Lossless or for Actively Changing Regions on Intel and AMD GPUs.

Limiting video resolutions

Administrators who have users on lower-performance client endpoints can choose to limit incoming or outgoing video resolutions to decrease the impact of encoding and decoding video on those endpoints. Starting from Citrix Workspace app 2010 for Windows, you can limit these resolutions using client configuration options.

Note:

Users running with restricted resolutions impact the overall video quality of the conference because the Microsoft Teams server will be forced to use the lowest-common-denominator resolution for all conference participants.

Call constraints are disabled by default on the client with Citrix Workspace app 2210. To enable, administrators must set the following client-side configurations in the HKEY_CURRENT_USER\SOFTWARE\Citrix\HDXMediaStream:

NAME	TYPE	MANDATORY	ACCEPTED VALUES
EnableSimulcast	Int	YES	1–3 (Set it to 1)
MaxOutgoingResolution	Int	YES	180,240,360,540,720,1080 (Microsoft Teams supported Resolutions)
MaxIncomingResolution	Int	YES	180,240,360,540,720,1080 (Microsoft Teams supported Resolutions)
MaxIncomingStreams	Int	YES	1–8
MaxSimulcastLayers	Int	YES	1–3 (set it to 1)
MaxVideoFrameRate	Int	NO	1–30
MaxScreenshareFrameRate	Int	NO	1–15

All keys are DWORDs.

Default audio device selection

Starting with the 2409 version of Citrix Workspace app, you can now select your preferred audio devices directly in the Desktop Viewer toolbar. This feature offers a more customized audio experience with the following key features when connected to a virtual desktop:

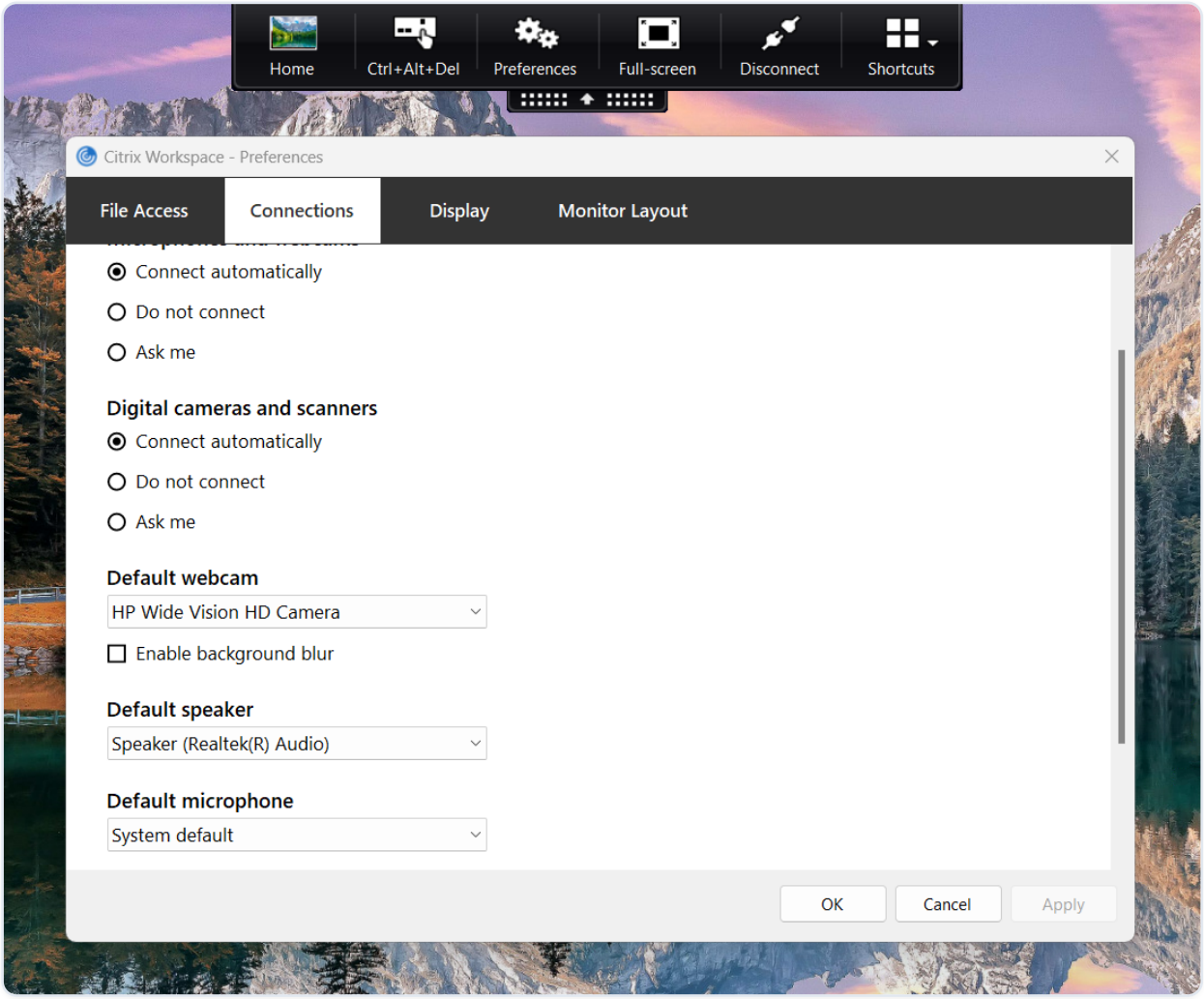
- **Device splitting**: You can assign different audio devices to different VDAs. For example, you can have two monitors with two different VDAs, each using a separate audio device (one loudspeaker and one headset).
- **Specific device selection**: The exact audio device can be selected for each active VDA from the **Preferences** section.
- **Configuration persistence**: The selected configuration is preserved for the next session, ensuring a seamless experience.

Note:

- If you do not want the selected configuration to be preserved for the next session, you can adjust the settings accordingly in the **Preferences** section.
- This feature isn't applicable to a pooled desktop environment because each time a user signs in, they might be connected to a different VDA.

To select the specific audio device, do the following:

1. Navigate to the **Preferences** section on the Desktop Viewer toolbar.
2. Click **Connections**. The following image appears:



3. Select the device that you want from the **Default speaker** drop-down list.
4. Select the device that you want from the **Default microphone** drop-down list.
5. Click **OK** to save the changes.

Loss tolerant mode for audio

Starting with 2311.1 release, Citrix Workspace app uses loss tolerant mode for audio redirection. This feature improves the user experience for real-time streaming when users are connecting through networks with high latency and packet loss.

You need to use VDA version 2311 or later. By default this feature is enabled on Citrix Workspace app for Windows. However, it is disabled on VDA.

To enable loss tolerant mode for audio, configure the following registry value and restart the machine.

For Multi-session VDA:

- Key: HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\Citrix\Audio
- Value name: EdtUnreliableAllowed
- Value type: DWORD
- Value data: 1

For Workstation VDA:

- Key: HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\Audio
- Value name: EdtUnreliableAllowed
- Value type: DWORD
- Value data: 1

Audio Quality Enhancer for EDT loss tolerant mode

Starting with the 2503.10 version, audio quality enhancer is enabled by default for adaptive audio over EDT loss tolerant mode for audio.

Audio quality enhancer maintains clear audio during brief network disruptions. This feature adapts to the network conditions to ensure consistent audio performance during playback and recording.

> **Note:**
>
> Adaptive audio must be enabled for this feature to work.

Enable noise suppression

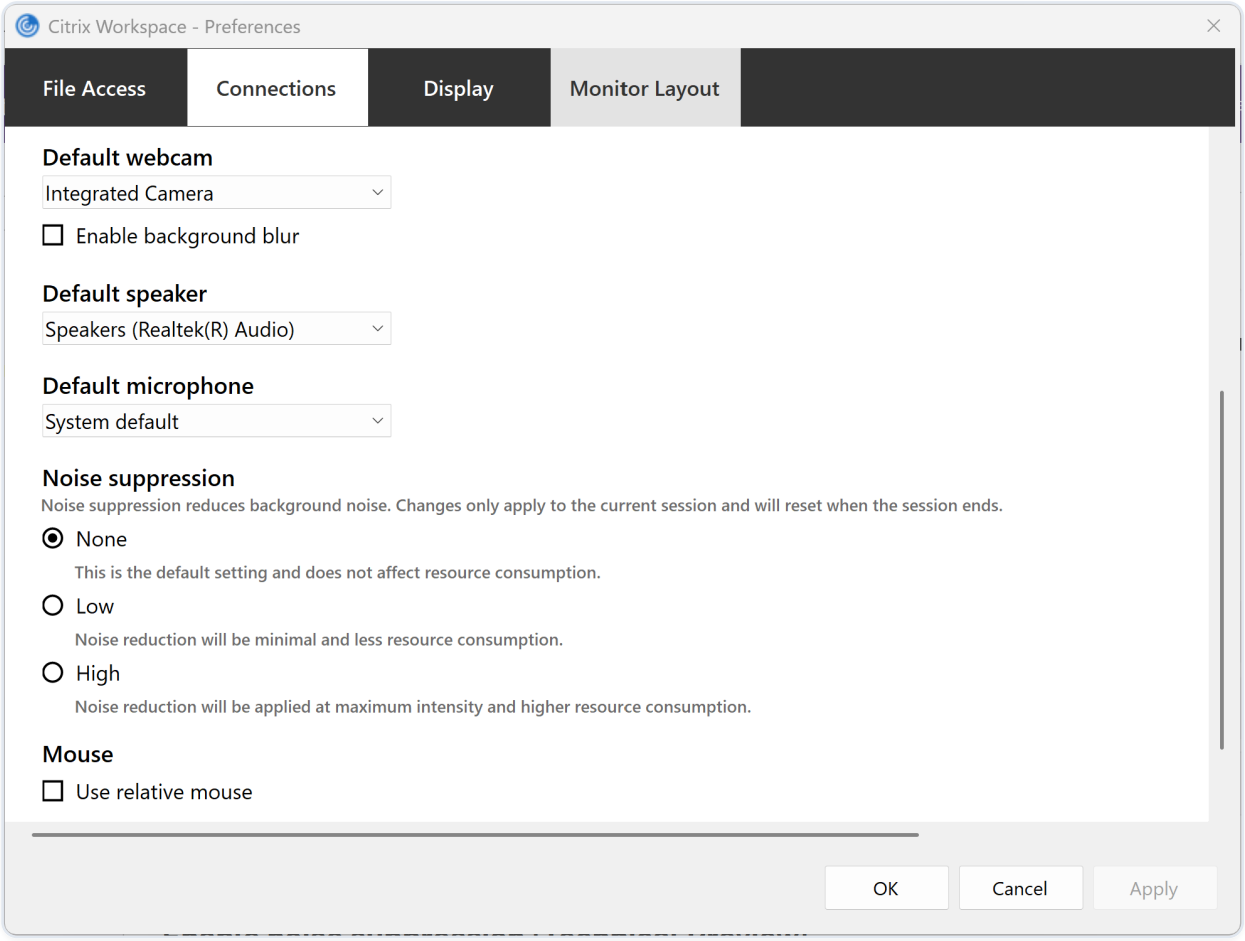
Starting with the 2507.1 version, Citrix Workspace™ app now offers improved audio redirection with enhanced noise suppression. This feature reduces background noise, ensuring clearer and more accurate speech, improving the overall communication experience.

Note:

This feature is disabled by default.

To enable this feature, do the following:

1. Navigate to the **Preferences** > **Connections** section. The Noise Suppression screen appears.



2. Select one of the following levels:

   - **None**: This level is the default setting and doesn't use or affect resource consumption.
   - **Low**: Noise reduction is minimal and uses the least resource consumption.
   - **High**: Noise reduction is applied at maximum intensity with the best performance and uses higher resource consumption than the Low setting.

3. Click **OK**. The selected configuration is applied.

Note:

Changes apply only to the current session and reset once the session ends.

Optimized Microsoft Teams

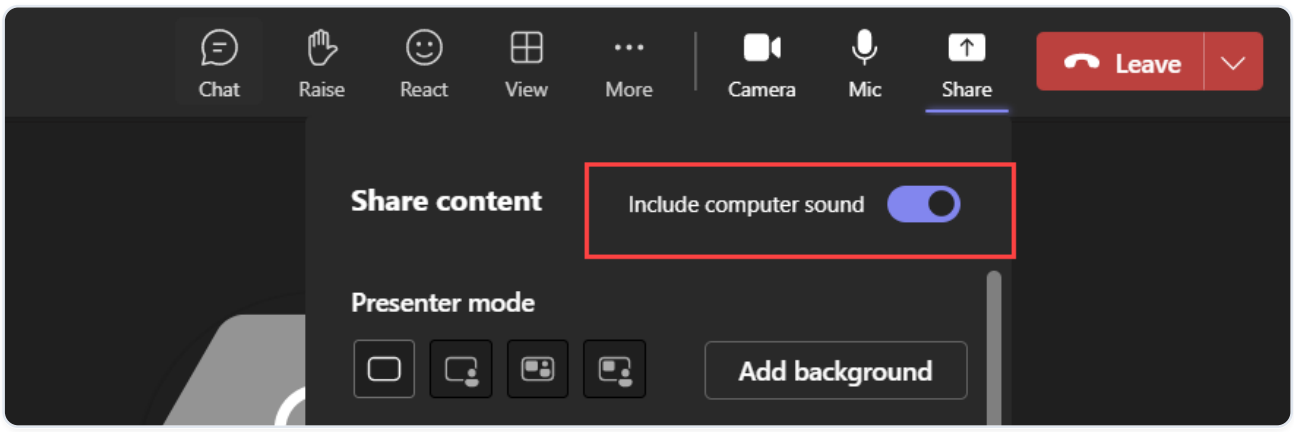
Improved audio performance in Microsoft Teams

Starting with the Citrix Workspace™ app for Windows version 2503, the audio subsystem used in the **HDXRTCMediaEngine** has been replaced with a newer system. As a result, Microsoft Teams now provides better audio performance, enhancing the overall user experience during calls and meetings. Along with this feature, the following issues related to Microsoft Teams optimization have been resolved:

- The new plug-in device might not be available in the **Microphone** drop-down menu option.
- Duplicate entries of devices might be present in the **Microphone** drop-down menu option.
- Users might not hear from the new plug-in headset when the default output devices (**Speakers/ Headphones**) on the client are disabled.
- Unplugging the last connected device might make the system unresponsive.

Share system audio

Starting with the Citrix Workspace app for Windows version 2405, you can share the audio playing on your VDA with participants in a meeting. Select the **Include computer sound** option to make your meetings more engaging. This feature is enabled by default. For end users, to use the feature, turn on **Include computer sound** on before sharing their screen.



Limitations:

- Audio cannot be shared using this feature when sharing the screen with RAVE and BCR redirected apps or tabs.
- This feature is supported only on published desktops.

Install Microsoft Teams VDI plug-in

Microsoft Teams VDI plug-in is the upcoming new VDI solution for Microsoft Teams. For more information, see the Microsoft documentation.

The difference between the Microsoft Teams (new or Classic) with VDI 1.0 optimization and Microsoft Teams (new) with VDI 2.0 optimization is as follows:

MICROSOFT TEAMS (NEW OR CLASSIC) WITH VDI 1.0 OPTIMIZATION	MICROSOFT TEAMS (NEW) WITH VDI 2.0 OPTIMIZATION
This version indicates that Microsoft Teams is optimized with Citrix HDX optimization, a combined solution between Microsoft and Citrix. In this case, the media engine (HdxRtcEngine) on the endpoint responsible for handling offloaded media is embedded in Citrix Workspace app and installing Citrix Workspace app automatically installs the media engine as well.	This version indicates that Microsoft Teams will be optimized with VDI 2.0 Optimization, a purely Microsoft solution built leveraging Citrix Virtual Channel SDK. This solution isn't generally available yet from Microsoft end. However, as this optimization needs a new engine (VDI 2.0) on the endpoint which will be responsible for handling offloaded media, Citrix is providing an easy way to deploy the Microsoft Teams plug-in. This plug-in, when installed, downloads the VDI 2.0 engine when it is generally available from Microsoft end.

You can install Microsoft Teams VDI plug-in during the installation of Citrix Workspace app using UI or using the command line.

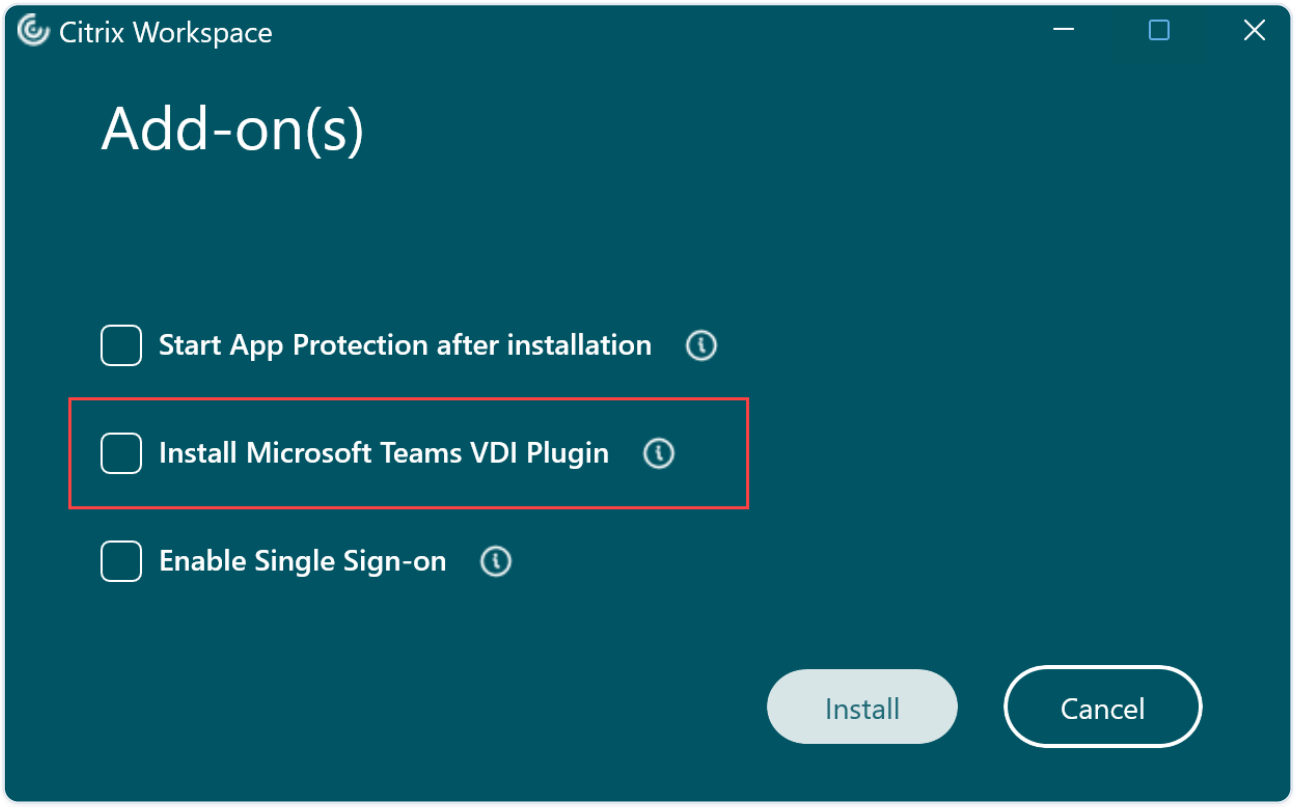
Note:

For version compatibility with VDI and configuration details, see Microsoft Teams 2.1 supported for VDI/DaaS and New Teams VDI requirements.

Using UI

1. On the **Add-on(s)** page, select the **Install Microsoft Teams VDI plug-in** checkbox, and then click **Install**.

2. Agree to the user agreement that pops up and proceed with the installation of Citrix Workspace app.



Using the command line

Use command line switch `/installMSTeamsPlugin`.

For example: `CitrixWorkspaceApp.exe /installMSTeamsPlugin`

Added support for playing short tones in optimized Microsoft Teams

Earlier, with the secondary ringtone feature enabled, short tones such as beeps or notifications were playing repeatedly. For example, the tone that was played when a guest joins the Microsoft Teams meeting was repeated. The only workaround was to quit and restart Microsoft Teams. This issue resulted in a poor end-user experience.

Starting with 2307 release, Citrix Workspace app supports playing the short tones as desired. This support also enables the secondary ringtone feature.

Prerequisites:

Update to the latest version of Microsoft Teams.

Support for WebHID API in UCSDK

Starting with the 2409 version, Citrix Workspace app for Windows supports the WebHID API to redirect Human Interface Device (HID) devices from an endpoint to Unified Communication SDK (UCSDK) integrated app on the VDI. It complies with the HID standard for bi-directional communication between the app that is integrated with UCSDK and the HID devices connected to the endpoint. With this feature, your UCSDK app interprets the **HID headset** commands such as Call accept, reject, mute, or unmute and so on in the HDX session for an enhanced user experience. This feature is enabled by default.

> **Note:**
>
> To take advantage of this feature, your real-time communications app must integrate UCSDK 4.0.

Improved experience for optimized Microsoft Teams video conference calls

Starting with Citrix Workspace app 2305 release, by default simulcast support is enabled for optimized Microsoft Teams video conference calls. With this support, the quality and experience of video conference calls across different endpoints are improved by adapting to the proper resolution for the best call experience for all callers.

With this improved experience, each user might deliver multiple video streams in different resolutions (for example, 720p, 360p, and so on) depending on several factors including endpoint capability, network conditions, and so on The receiving endpoint then requests the maximum quality resolution that it can handle thereby giving all users the optimum video experience.

Background blurring and effects for Microsoft Teams optimization with HDX™

Citrix Workspace app for Windows now supports background blurring and effects in Microsoft Teams optimization with HDX.

You can either blur or replace the background with a custom image and avoid unexpected distractions by helping the conversation stay focused on the silhouette (body and face). The feature can be used with either P2P or conference calls.

Starting with Citrix Workspace app for Windows version 2311.1, you can select the following options for background blurring and effects:

- No background effect
- Select Background Blurring
- Select Background Image

> **Note:**
>
> This feature is now integrated with the Microsoft Teams UI/buttons. MultiWindow support is a prerequisite that requires a VDA update to 2112 or higher. For more information, see Multi-window meetings and chat.

> **Limitations:**

- User-defined background replacement is not supported.
- The background effect doesn't persist between sessions. When you close and relaunch Microsoft Teams or VDA is reconnected, the background effect is reset to off.
- After the ICA® session is reconnected, the effect is off. However, the Microsoft Teams UI shows that the previous effect is still On by a tick mark. Citrix® and Microsoft are working together to resolve this issue.
- The device must be connected to the internet while replacing the background image.

> **Note:**
>
> This feature is available only after future update roll-out from Microsoft Teams. When the update is rolled-out by Microsoft, you can check CTX253754 and the Microsoft 365 Public roadmap for the documentation update and the announcement.

Acoustic Echo Cancellation

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

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

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

Enhancements to Microsoft Teams optimization

- Starting from Citrix Workspace app 2209 for Windows:
  - The version of WebRTC that is used for the optimized Microsoft Teams is upgraded to version M98.
- Starting from Citrix Workspace app 2302 for Windows:
  - **Updated audio device selection behavior for optimized Microsoft Teams** - When you change the default audio devices in the sound settings on the endpoint, the optimized Microsoft Teams in the Citrix VDI changes the current audio devices selection to match the endpoint defaults.

    However, if you make an explicit device selection in Microsoft Teams, your selection takes precedence and does not follow the endpoint defaults. Your selection is persistent until you clear the Microsoft Teams cache.

For information on features that were part of releases which reached End of Life (EOL), see Legacy documentation.

HDX™ transport

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.

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

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

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

Important:

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

Adaptive transport

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

Browser Content Redirection

Introduction

Browser Content Redirection (BCR) enhances the user experience of web browsing within Citrix Virtual Apps and Desktops™ environments. By rendering webpages on the user's local machine, BCR reduces server load and improves performance, especially for complex or resource-intensive websites.

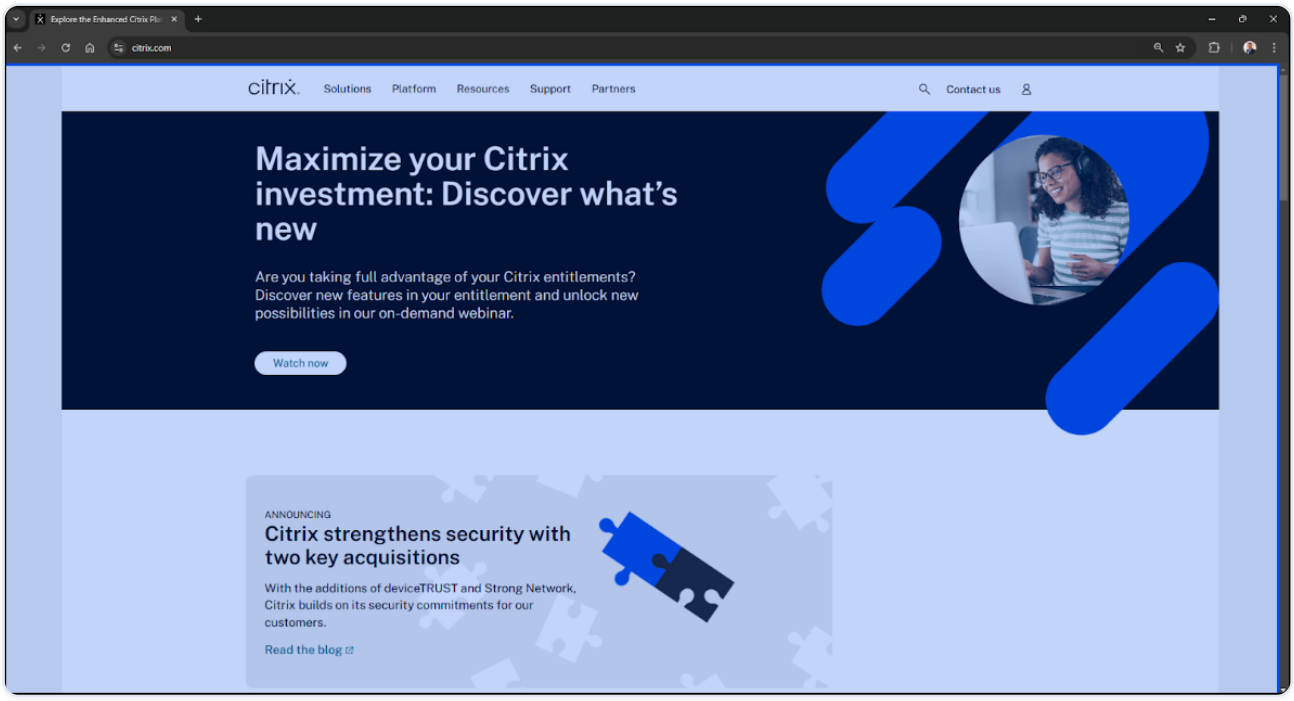
For more information about the feature, see the Citrix Virtual Apps and Desktops documentation. On Windows clients, Browser Content Redirection uses the Chromium-Embedded Framework as the browser overlay engine.

Functionality overview

BCR uses the Citrix Workspace™ app to create a secure browsing environment on the user's device. When a user accesses an allowed webpage, the viewport of the browser window is redirected to the client. The client-side browser engine then uses the local machine's resources to render the page, resulting in faster loading times and smoother interaction.

Only the browser viewport is redirected. The viewport is the rectangular area in your browser where the content is displayed. It does not include elements such as the Address Bar, Favorites Toolbar, or Status Bar. Those items remain part of the user interface, which continues to run on the browser in the VDA.

The blue highlighted area in the following image is the viewport:



Key benefits

Browser content redirection intelligently manages web traffic, delivering a superior experience for your users while reducing strain on your infrastructure. Here's how it can benefit your organization:

- **Cost savings**: Redirect resource-intensive webpages to user devices, freeing up valuable server resources and reducing bandwidth consumption. This translates to lower hardware and network costs.
- **Enhanced user experience**: Provide your users with a smoother, more responsive browsing experience, even with graphics-intensive websites. Deliver native-like performance, eliminating lag and improving productivity.
- **Improved security**: Maintain a secure environment while allowing access to both internal and external resources.
- **Increased flexibility**: Support a wide range of use cases, from basic web browsing to complex web applications that require proxy traversal or Single sign-on (SSO) authentication. Easily manage redirection settings with granular policy controls in Citrix Web Studio.

System requirements

Server side components

Citrix Virtual Apps and Desktops

Long Term Service Release:

- Minimum requirements: Any non end-of-life LTSR Citrix Virtual Apps and Desktops release
- Recommended: Citrix Virtual Apps and Desktops 2402 or above

Current Release:

- Minimum requirement: Any non end-of-life CR Citrix Virtual Apps and Desktops release
- Recommended: Latest Citrix Virtual Apps and Desktops release

Browser components

Browsers:

- Microsoft Edge
- Google Chrome

Browser redirection extension: Published in both Chrome and Edge web stores

We recommend using the latest version of the browsers for the best experience.

Client side components

Windows:

- Windows 10 or 11

Citrix Workspace app:

- Minimum requirement: Any non end-of-life Citrix Workspace app
- Recommended:
  - Long Term Service Release: Citrix Workspace app 2402 or latest CU
  - Current Release: Citrix Workspace app 2405 or above

> **Notes:**

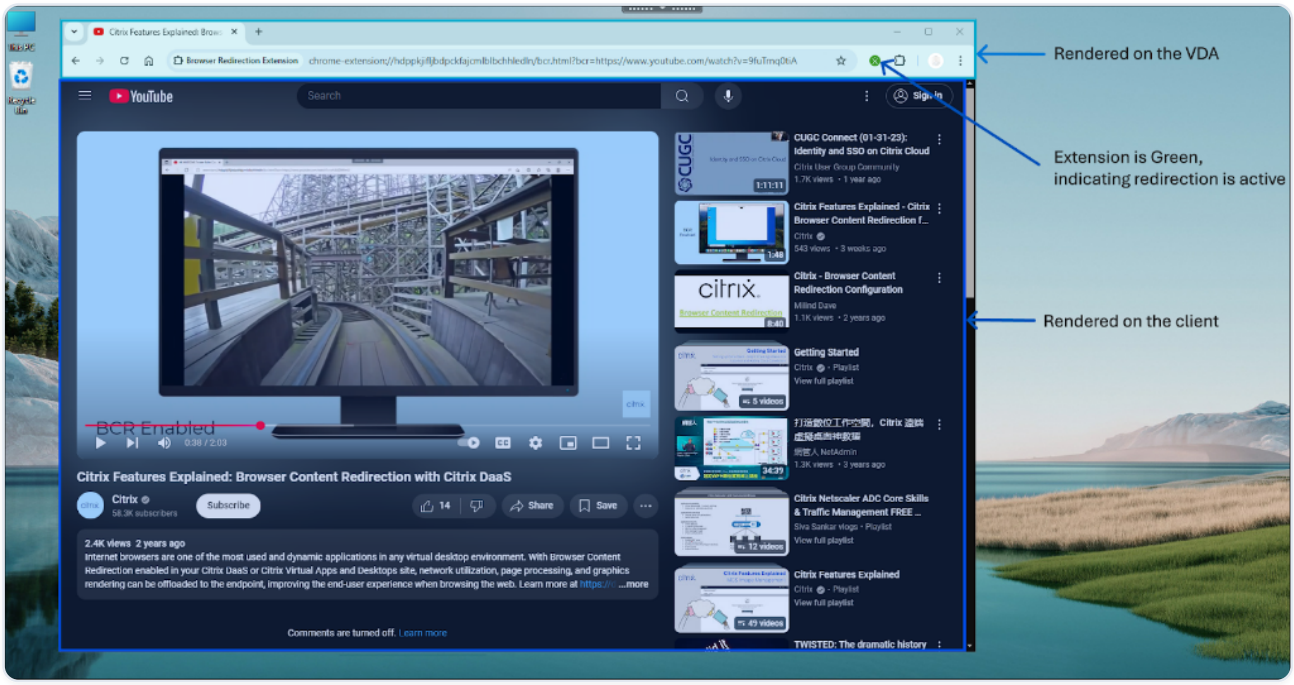
> - Browser content redirection is not supported on Citrix Workspace app for Windows LTSR releases 1912 and 2203.1
> - Client-side browser engine needed for Browser content redirection is installed by default on Citrix Workspace app Current Releases

- Client-side browser engine needed for Browser content redirection is not installed by default on Citrix Workspace app 2402 LTSR release. Administrators can use the ADDLOCAL switch to install BCR browser components on top of Citrix Workspace app. For more information, see the ADDLOCAL documentation.

Steps to configure

1. Install the client-side and server-side components according to the system requirements. For details on extension deployment, see the Extension deployment section.
2. Configure the studio policies:
    - Web studio policies offer a granular way to configure Browser content redirection to suit various use cases.
    - The basic policies allow the administrator to configure URLs that must be allowed or not allowed with Browser content redirection.
    - The URLs can be configured with wildcards.
3. Open a supported web browser and navigate to an allowed URL:
    - If the match is found in the allow list, the website is redirected to the client.
    - Citrix Workspace app integrates the viewport with the VDA side browser for a seamless experience.
    - The color of the extension logo specifies the status of the content redirection:
        - Green: Active and connected
        - Gray: Not active or idle on the current tab
        - Red: Broken or not working

The following image shows an example of a website rendered using BCR:



For more information on configuration options, see Browser content redirection policy settings.

Notes:

- HTML5 video redirection and browser content redirection are independent features. The HTML5 video redirection policies aren't needed for the BCR feature to function. However, the Citrix HDX™ HTML5 Video Redirection Service is used for BCR.
- Citrix recommends performing all configurations through Web Studio rather than using registry keys.

Modular Browser Content Redirection

Starting with the Citrix Workspace app 2507.1 for Windows, the Browser Content Redirection (BCR) component is now managed as a modular component, separate from the main Citrix Workspace app installer.

This new modular and evergreen model allows the Browser Content Redirection component to be updated independently and uninstalled independently. This feature provides the following key benefits:

- **Enhanced security**: The BCR Chromium Embedded Framework component can receive security patches and updates as soon as they are available, without waiting for a full Citrix Workspace app release.

- **Simplified Management**: Customers no longer need to update entire Citrix Workspace app to receive the latest Browser content redirection features.
- **Accelerated Innovation**: Faster deployment of new BCR features, enhancements, and bug fixes is now possible, delivering continuous value to customers

To ensure a consistent user experience, the Modular BCR component is installed by default in Citrix Workspace app.

Installation and management

When you install or upgrade to Citrix Workspace app 2507.1 or later, the installer includes the latest BCR component and installs it by default. No additional action is needed to install the BCR component.

For environments that do not use Browser Content Redirection, you can prevent its installation using the ADDLOCAL command-line switch during setup. When specifying ADDLOCAL components, do not include "BCR Client" to prevent BCR installation. For more information, see the Install and Uninstall section.

Manual installation and uninstallation

- **To install**: If you exclude the BCR component during initial setup, you can install it anytime by downloading the standalone installer from the Citrix Downloads page.
- **To uninstall**: The BCR component can be uninstalled separately from Citrix Workspace app anytime by uninstalling the Citrix Browser Content Redirection Plug-in from the Windows Settings > Apps >Installed Apps section.

Automatic updates:

Once the modular and evergreen BCR component is installed, it keeps itself up-to-date automatically. The component periodically checks for new versions and silently installs them in the background. This automatic update ensures you always have the latest features and security updates without manual upgrades.

> **Note:**
>
> Once you upgrade Citrix Workspace app to 2507.1 LTSR or later Current Releases, the BCR experience is consistent across releases. There is only one BCR package regardless of Current Release or LTSR.

Upgrading to Citrix Workspace app 2507.1

The transition from the older, integrated BCR is designed to be seamless. When you upgrade an existing Citrix Workspace app version to 2507.1 or later, the installer automatically replaces the old component with the new modular version. Users continue to have Browser Content Redirection functionality without any change to their experience.

> **Note:**
>
> In Citrix Workspace app 2402 LTSR, the BCR component was not installed by default. With Citrix Workspace app 2507.1 LTSR, BCR has undergone significant user experience improvements and is now installed by default.

Bidirectional content redirection

Bidirectional content redirection allows HTTP or HTTPS URLs in web browsers, or embedded into applications, to be forwarded between the Citrix VDA session and the client endpoint in both directions. This means:

- A URL entered in a browser running in the Citrix session can be opened using the client's default browser.
- Conversely, a URL entered in a browser running on the client can be opened in a Citrix session, either with a published application or desktop.

Citrix also offers host to client redirection and Local App Access redirection. However, it is recommended to use Bidirectional Content Redirection for most use cases.

> **Note:**
>
> For optimal performance of the Bidirectional Content Redirection feature, it is recommended to use Citrix Workspace app for Windows version 2311.1 or later. For LTSR, use version 2402 or later.

> For more information, see Bidirectional content redirection.

Configuration

From Citrix Workspace app for Windows 2311.1:

Prerequisites:

- Citrix Virtual Apps and Desktops™ version 2311 or later
- Citrix Workspace app for Windows 2311.1 or later

Starting with Citrix Workspace app for Windows 2311.1, bidirectional content redirection is configured entirely through Citrix Studio. For configuration details, see the Bidirectional content redirection documentation for Citrix Virtual Apps and Desktops.

> **Note:**
>
> It is recommended to use the new Citrix Virtual Apps and Desktops Version 2402 Web Studio or later to configure the Bidirectional Content Redirection policy. For more information, see Manage deployments documentation.

> **Before Citrix Workspace app for Windows 2311.1:**

When you are using versions before Citrix Virtual Apps and Desktops version 2311, you need to set server policies in Studio and set client policies using the Citrix Workspace app Group Policy Object administration template.

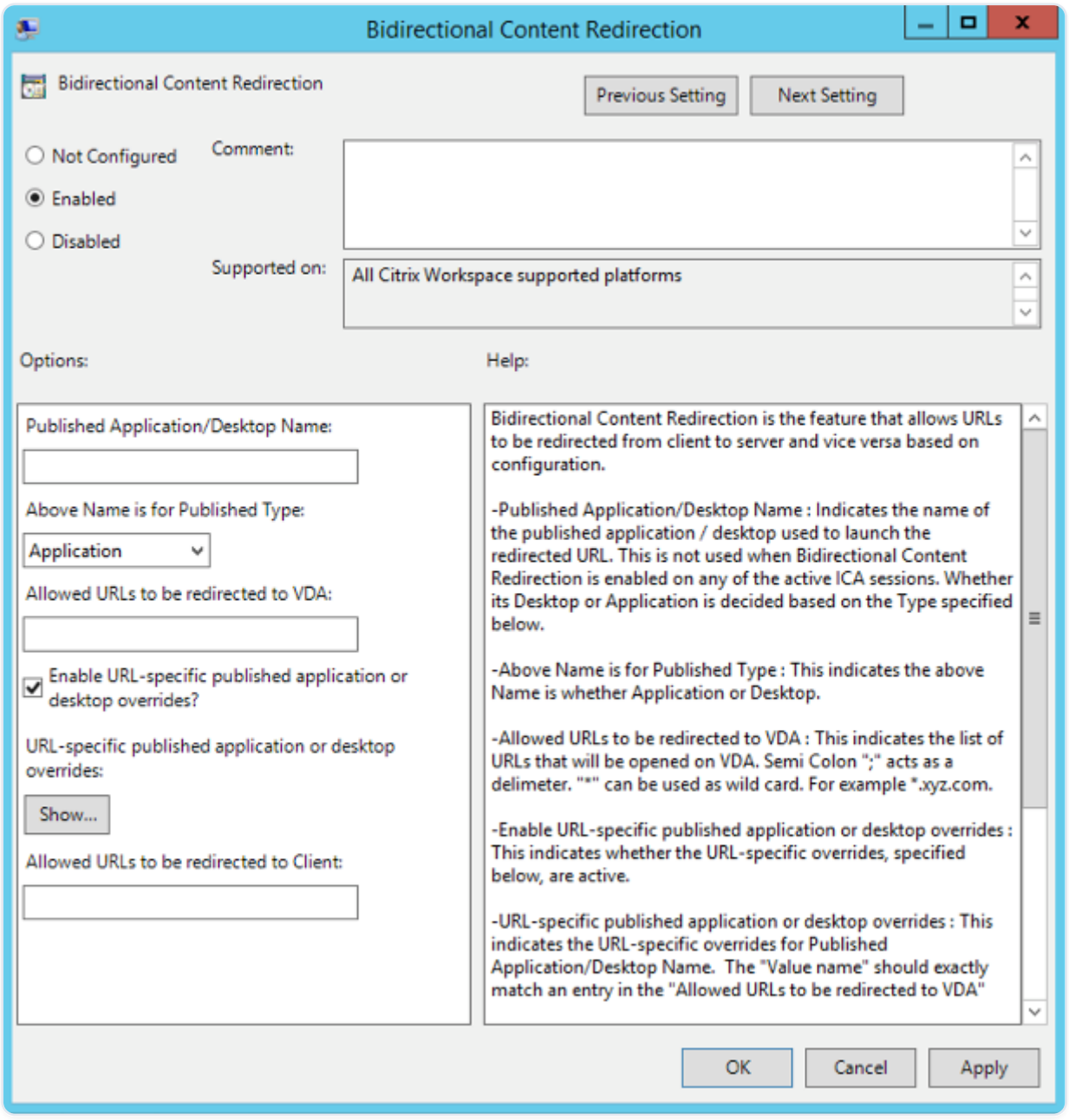
You can enable bidirectional content redirection using the Group Policy Object (GPO) administrative template.

> **Note:**
>
> - Bidirectional content redirection does not work on the session where **Local App Access** is enabled.
> - Bidirectional content redirection must be enabled both on the server and the client. When it is disabled either on the server or the client, the functionality is disabled.
> - When you include URLs, you can specify one URL or a semi-colon delimited list of URLs. You can use an asterisk (*) as a wildcard.

> **To enable bidirectional content redirection using the GPO administrative template:**

Use Group Policy Object administrative template configuration only for a first-time installation of Citrix Workspace app for Windows.

1. Open the Citrix Workspace app Group Policy Object administrative template by running gpedit.msc.
2. Under the **User Configuration** node, go to **Administrative Templates** > **Classic Administrative Templates (ADM)** > **Citrix Components** > **Citrix Workspace** > **User experience**.
3. Select the **Bidirectional Content Redirection** policy.

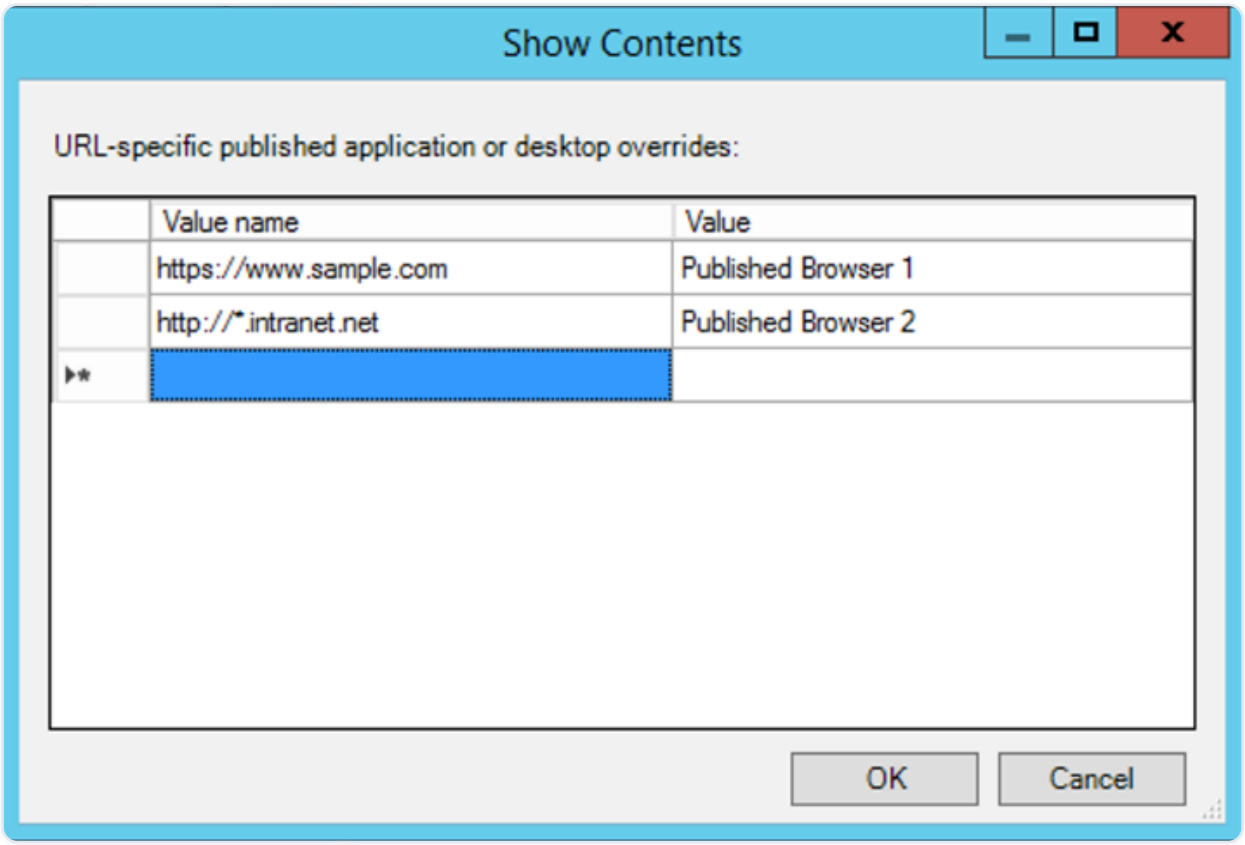


4. In the **Published Application or Desktop name** field, provide the name of the resource used to launch the redirected URL.

Note:

When you include URLs, specify a single URL or a semi-colon delimited list of URLs. You can use an asterisk (*) as a wildcard.

5. From the **Above Name is for Published Type**, select **Application** or **Desktop** of the resource as appropriate.
6. In the **Allowed URLs to be redirected to VDA** field, enter the URL that must be redirected. Separate the list with a semicolon.
7. Select the **Enable URL-specific published application for desktop overrides?** option to override a URL.
8. Click **Show** to display a list where the value name must match any of the URLs listed in the **Allowed URLs to be redirected to the VDA** field. The value must match a published application name.



9. In the **Allowed URLs to be redirected to Client:** field, enter the URL that must be redirected from the server to the client. Separate the list with a semicolon.

Note:

> When you include URLs, specify a single URL or a semi-colon delimited list of URLs. You can use an asterisk (*) as a wildcard.

10. Click **Apply** and then **OK**.
11. From the command line, run the `gpupdate /force` command.

Limitation:

- No fallback mechanism is present if the redirection fails due to session launch issues.
- When performing client-to-host redirection to a published application, ensure that the published application is set as the default browser. If it is not, bidirectional redirection might not work as expected.

ICA Settings Reference

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

ICA Settings Reference (PDF download)

Devices

This section describes the configuration settings for the following:

- Mouse
- Keyboard
- Printing
- USB
- Webcams
- Client drive-mapping
- Microphone
- Audio

Mouse

Relative mouse

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

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

You can configure the feature both on a per-user and a per-session basis, which gives more granular control on the feature availability.

> **Note**

> This feature can be applied in a published desktop session only.

> Configuring the feature using the Registry Editor or the default.ica file allows the setting to be persistent even after the session is terminated.

Configuring relative mouse using the Registry editor

To configure the feature, set the following registry keys as applicable and then restart the session for the changes to take effect:

To make the feature available on a per-session basis:

`HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Citrix\ICA Client\Engine\Lockdown Profiles\All Regions\Lockdown\Virtual Channels\RelativeMouse`

To make the feature available on a per-user basis:

`HKEY_CURRENT_USER\Software\Policies\Citrix\ICA Client\Engine\Lockdown Profiles\All Regions\Lockdown\Virtual Channels\RelativeMouse`

- Name: Mouse
- Type: REG_SZ
- Value: True

> **Note:**
>
> - The values set in the Registry editor take precedence over the ICA® file settings.
> - The values set in HKEY_LOCAL_MACHINE and HKEY_CURRENT_USER must be the same. Different values might cause conflicts.

Configuring the relative mouse using the default.ica file

1. Open the default.ica file typically at `C:\inetpub\wwwroot\Citrix\<site name>\conf\default.ica`, where sitename is the name specified for the site while creating. For StoreFront customers, the default.ica file is typically at `C:\inetpub\wwwroot\Citrix\<Storename>\App_Data\default.ica`, where `storename` is the name set for the store when created.
2. Add a key by name RelativeMouse in the WFClient section. Set its value to the same configuration as the JSON object.
3. Set the value as required:

- true – To enable relative mouse
- false – To disable relative mouse

4. Restart the session for the changes to take effect.

> **Note:**
>
> The values set in the Registry editor take precedence over the ICA file settings.

Enabling relative mouse

You can enable relative mouse using shortcut key or from the Desktop Viewer.

Enable relative mouse using shortcut key for Relative mouse

You can use Ctrl+F12 key to turn on or off the Relative Mouse. However, you can modify this shortcut key to a different shortcut or you can disable the shortcut. For more information, see Keyboard shortcuts.

Enabling relative mouse from the Desktop Viewer

1. Log on to Citrix Workspace app.
2. Launch a published desktop session.
3. From the Desktop Viewer toolbar, select **Preferences**.

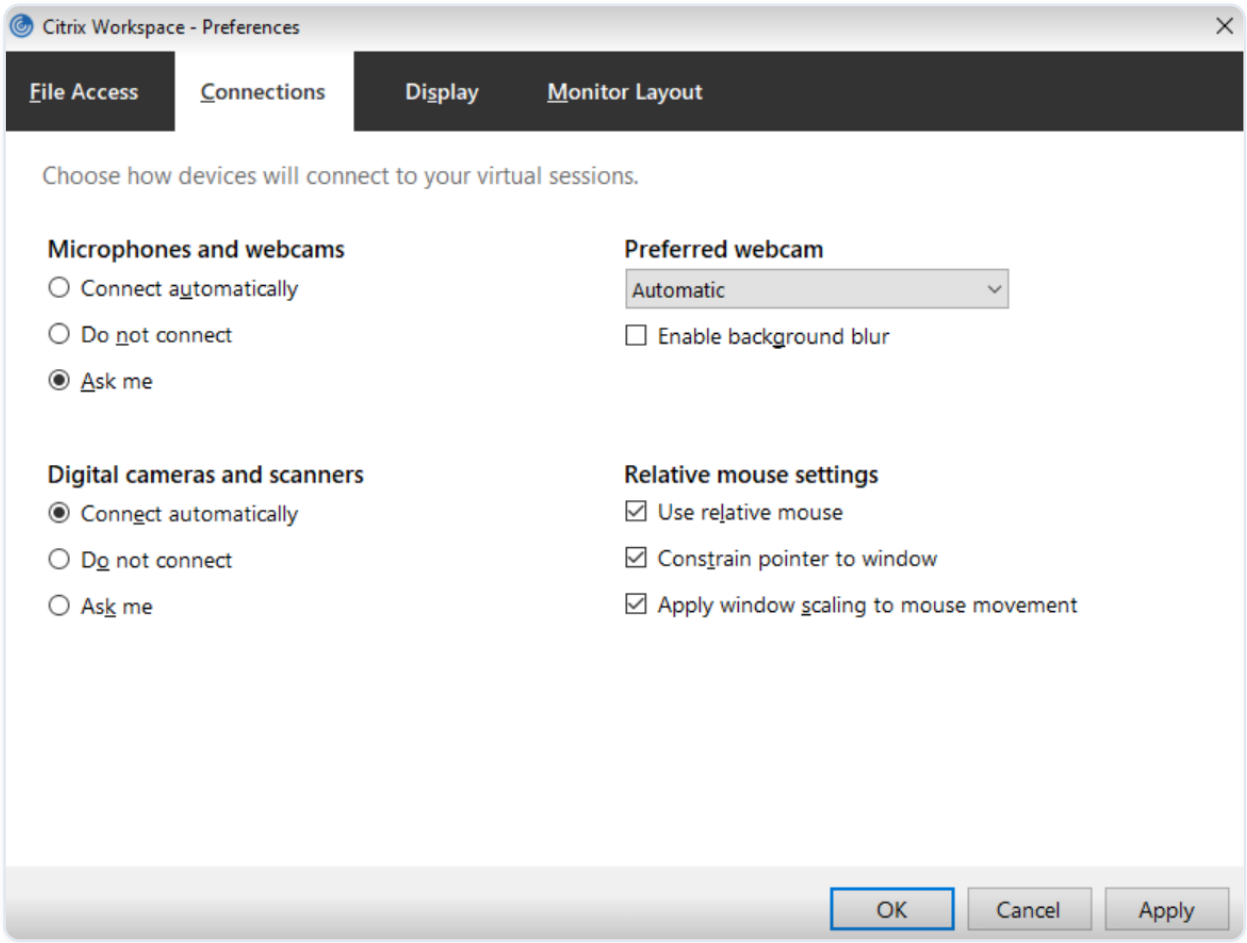
   The Citrix Workspace - Preferences window appears.
4. Select **Connections**.
5. Under **Relative Mouse** settings, enable **Use relative mouse**.
6. Click **Apply** and **OK.**

> **Note:**
>
> Configuring the relative mouse from the Desktop Viewer applies the feature to per-session only.

Enhancement to relative mouse

Starting with Citrix Workspace app for Windows 2405 version, you can restrict the usage of mouse to the window using the preferences UI available from the toolbar. This enhancement helps you to use the apps that need to monitor mouse movement extending to or beyond the boundaries of the virtual desktop's screen. These apps include third-party apps or those apps that scroll a view in response to mouse movement. To use this feature, do the following:

1. Ensure that relative mouse is enabled. For more information, see Enabling relative mouse.
2. Select the **Constrain pointer to window** checkbox.

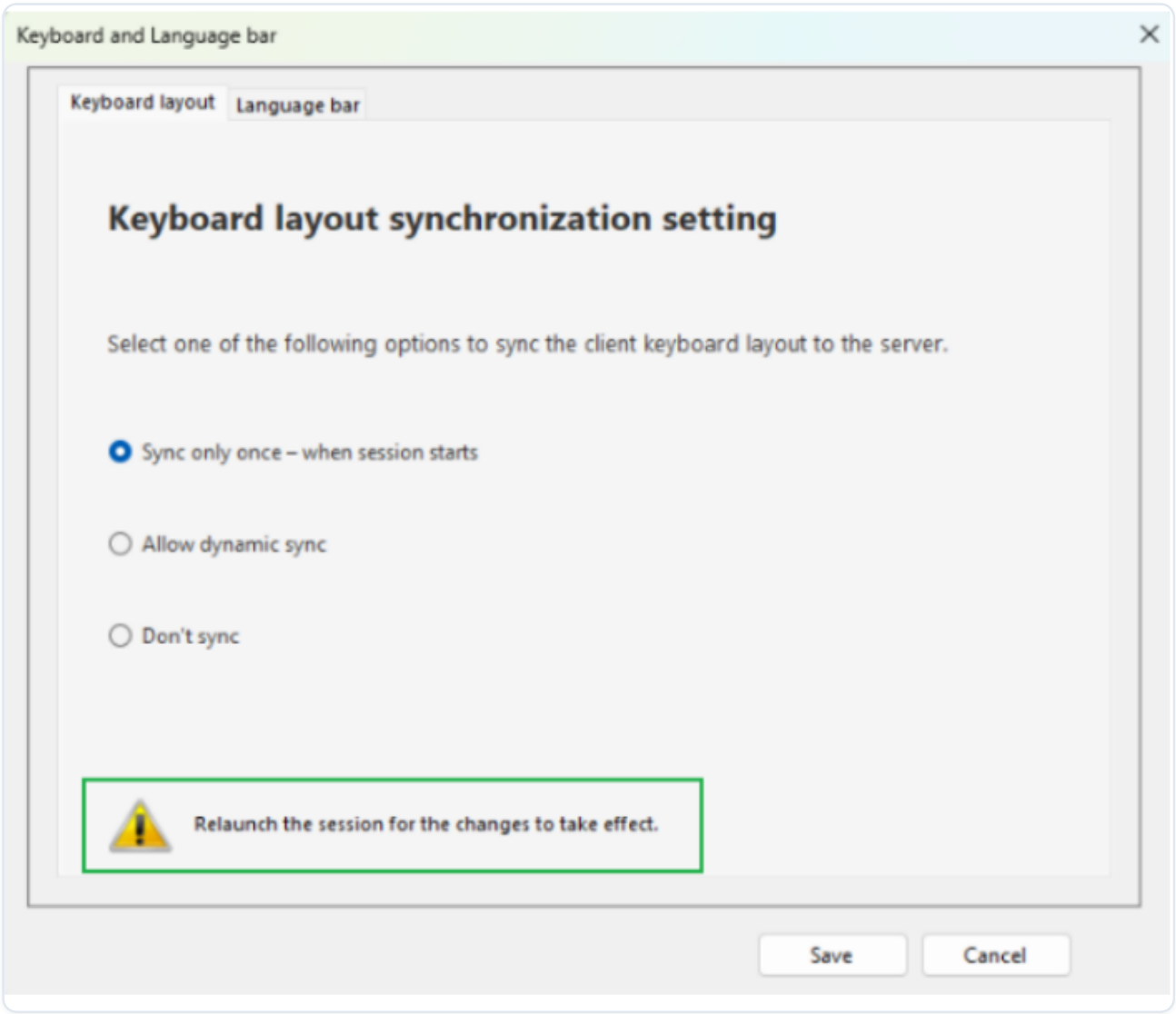


3. Click **Apply** and then click **OK**.

Keyboard

Enhanced keyboard layout settings notification

Starting with this release, the keyboard layout settings UI displays a warning that informs you that a session relaunch is required for changes to take effect.



Keyboard shortcuts

Citrix Workspace app for Windows passes most keys combinations through to the virtual app or desktop. However, by default it uses certain keyboard shortcuts to provide special functionality. These keyboard shortcuts apply to apps and desktops where the Desktop Viewer toolbar is disabled.

> **Important:**

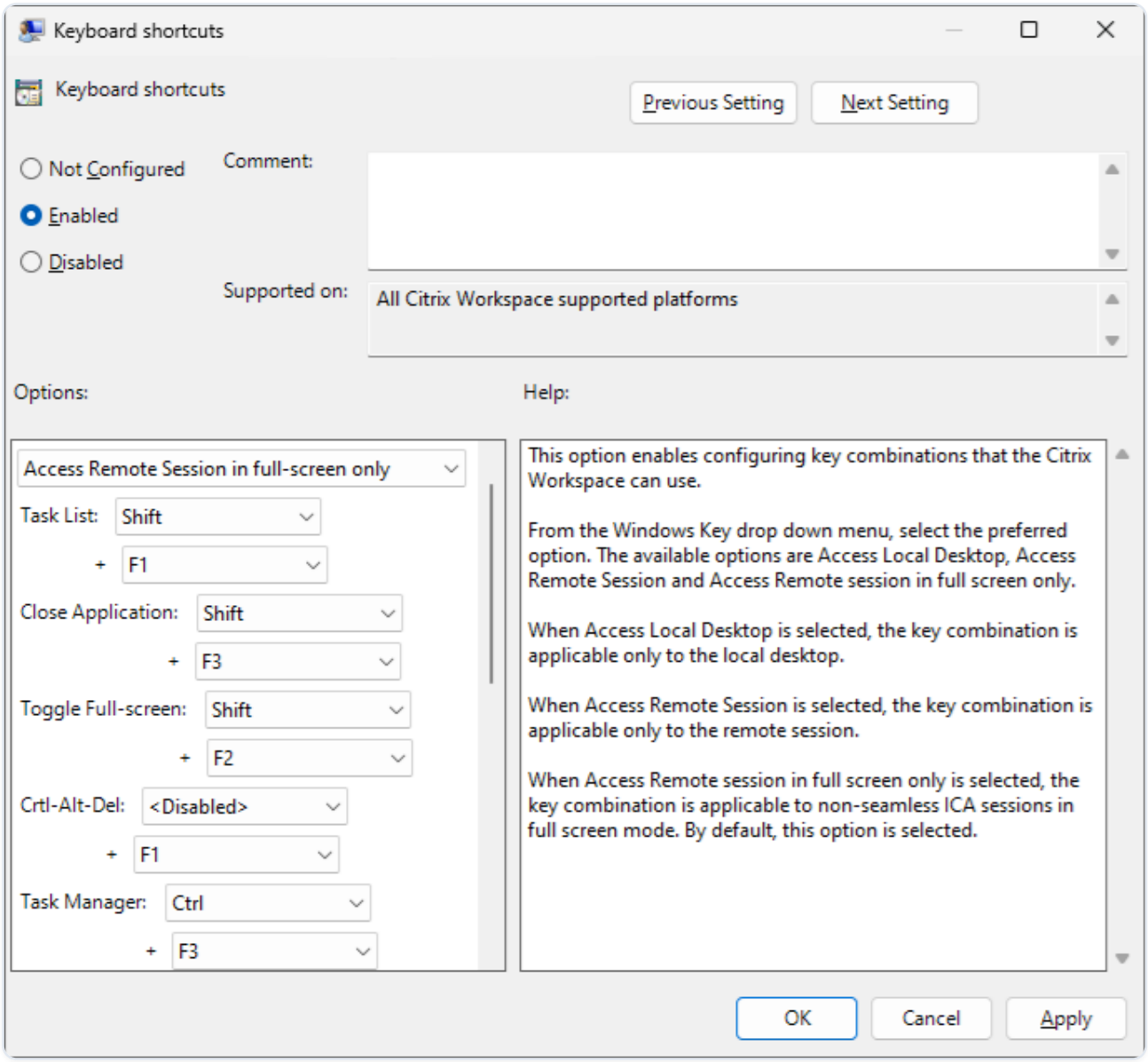
> These shortcuts do not apply if the Desktop Viewer is enabled, instead see Keyboard shortcuts for Desktop Viewer.

NUMBER	DEFAULT SHORTCUT	FUNCTION	APPLIES TO
1	Shift+F1	Invoke the Windows key locally to bring up the start menu	Apps and desktops
2	Shift+F3	Close Citrix® session window	Apps and desktops
3	Shift+F2	For apps, toggle between seamless and windowed mode. For desktop toggle between full-screen and windowed mode.	Apps and desktops
4	Ctrl+F1	Invoke Ctrl+Alt+Delete	Apps and desktops
5	Ctrl+F3	Open task manager	Apps and desktops
6	Alt+F8	Invoke Alt+Tab (task switcher).	Desktops
7	Alt+F9	Invoke Shift+Alt+Tab (reverse task switcher).	Desktops
8	Ctrl+F2	Invoke Ctrl+Esc (in desktops opens the Start menu).	Apps and desktops
9	Alt+F2	Invoke Alt+Esc (switch windows).	Apps and desktops
10	n/a	Previously Ctrl+F5 enabled Latency	

NUMBER	DEFAULT SHORTCUT	FUNCTION	APPLIES TO
		Reduction. No longer applies.	
11	n/a	Reserved	
12	n/a	Reserved	
13	Shift+F11	Minimizes the session window.	Desktops
14	Shift+F4	Toggle IME mode. Only relevant when IME is configured.	Desktops
15	Ctrl+F12	Relative Mouse.	Apps and Desktops

You might find that these shortcuts clash with shortcuts used by your virtual apps. If this happens then you can either assign a different shortcut or disable the shortcut. To configure shortcut keys using Group Policy:

1. Open the Citrix Workspace app Group Policy Object administrative template by running gpedit.msc.
2. Under the **Computer Configuration node**, go to **Administrative Templates**\> **Citrix Components** \> **Citrix Workspace** \> **User Experience**.
3. Select the **Keyboard shortcuts** policy.
4. Select **Enabled**
5. Updated the options as required and press **OK**.
6. Restart the Citrix Workspace app session for the changes to take effect.



Alternatively you can configure keyboard shortcuts in StoreFront by editing the Default.ica. See Configure session settings. In the `[WFCLIENT]` section, for each hotkey add two entries:

KEY	VALUE
Hotkey{n}Char	F1/F2/F3/F4/F5/F6/F7/F8/F9/F10/F11/F12/ minus/plus/star/tab
Hotkey{n}Shift	Ctrl/Shift/Alt

For example to configure shortcut 2, which is close Citrix session window, to use Alt+F3 instead of Shift+F3, add:

```
Hotkey2Char=F3

Hotkey2Shift=Alt
```

To disable shortcut 2, so the default shortcut Shift+F3 is passed through to the VDA, without an alternative shortcut:

```
Hotkey2Char=

Hotkey2Shift=
```

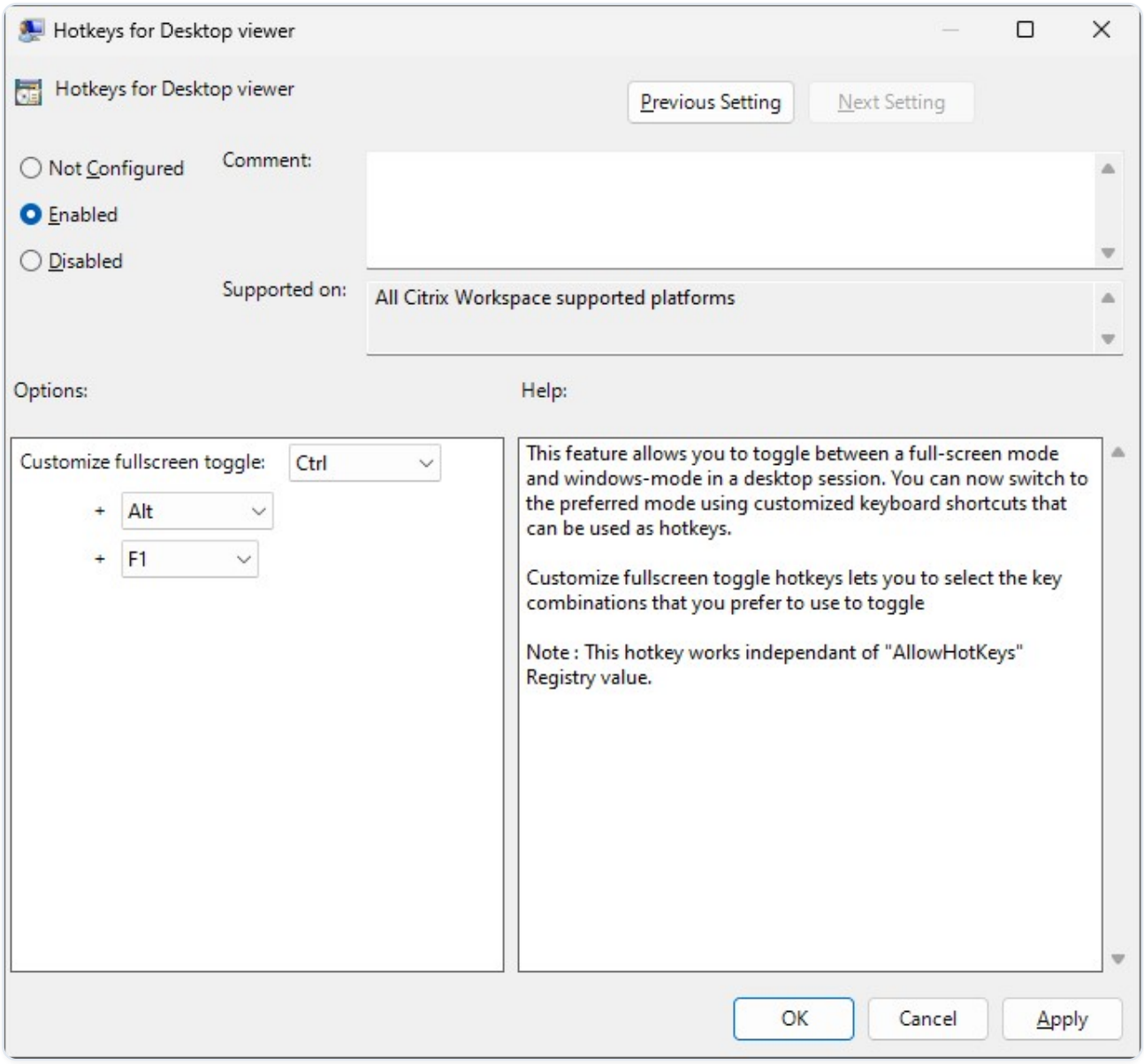
Keyboard shortcuts for Desktop Viewer

Normally Citrix Workspace app passes all keys through to the virtual app or desktop. However, by default certain keyboard shortcuts that provide special functionality. These shortcuts apply only when using the Desktop Viewer. If you have disabled the Desktop Viewer then see Keyboard shortcuts.

DEFAULT SHORTCUT	FUNCTION	
Ctrl+Alt+F1	Toggle between full-screen and window	
Ctrl+Alt+Break	Open the context menu of the desktop session	

You can customize (but not remove) the shortcut for the fullscreen toggle by using Group Policy. It is not possible to customize the shortcut for opening the context menu.

1. Open the Citrix Workspace app Group Policy Object administrative template by running gpedit.msc.
2. Under the **Computer Configuration node**, go to **Administrative Templates**\> **Citrix Components** \> **Citrix Workspace** \> **User Experience**.
3. Select the **Hotkeys for Desktop viewer** policy.
4. Select **Enabled**.
5. Update the settings as required and press **OK**.
6. Restart the Citrix Workspace app session for the changes to take effect.



Passing Windows shortcut keys to the remote session

Most Windows shortcut keys function within the remote session, except for Windows+L. Frequently used examples include:

- **Win+D**: Minimize all open windows.
- **Win+U**: Open the **Settings** app to the **Accessibility** section.
- **Alt+Tab**: Switch between active windows.
- **Ctrl+Alt+Delete**: Accessible via Ctrl+F1 or the Desktop Viewer toolbar.
- **Alt+Shift+Tab**: Navigate backward through active windows.
- **Windows+Tab**: Open the Task view.
- **Windows+Shift+Tab**: Navigate backward through the Task view.

- **Windows+All Character Keys**: Various shortcuts based on the specific character key.

> **Note:**
>
> Starting with Citrix Workspace™ app for Windows 2503 and later versions, "Windows + U" shortcut works within remote sessions launched in full-screen mode. In previous versions of Citrix Workspace app, this shortcut works locally.

Keyboard layout and language bar

Keyboard layout

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

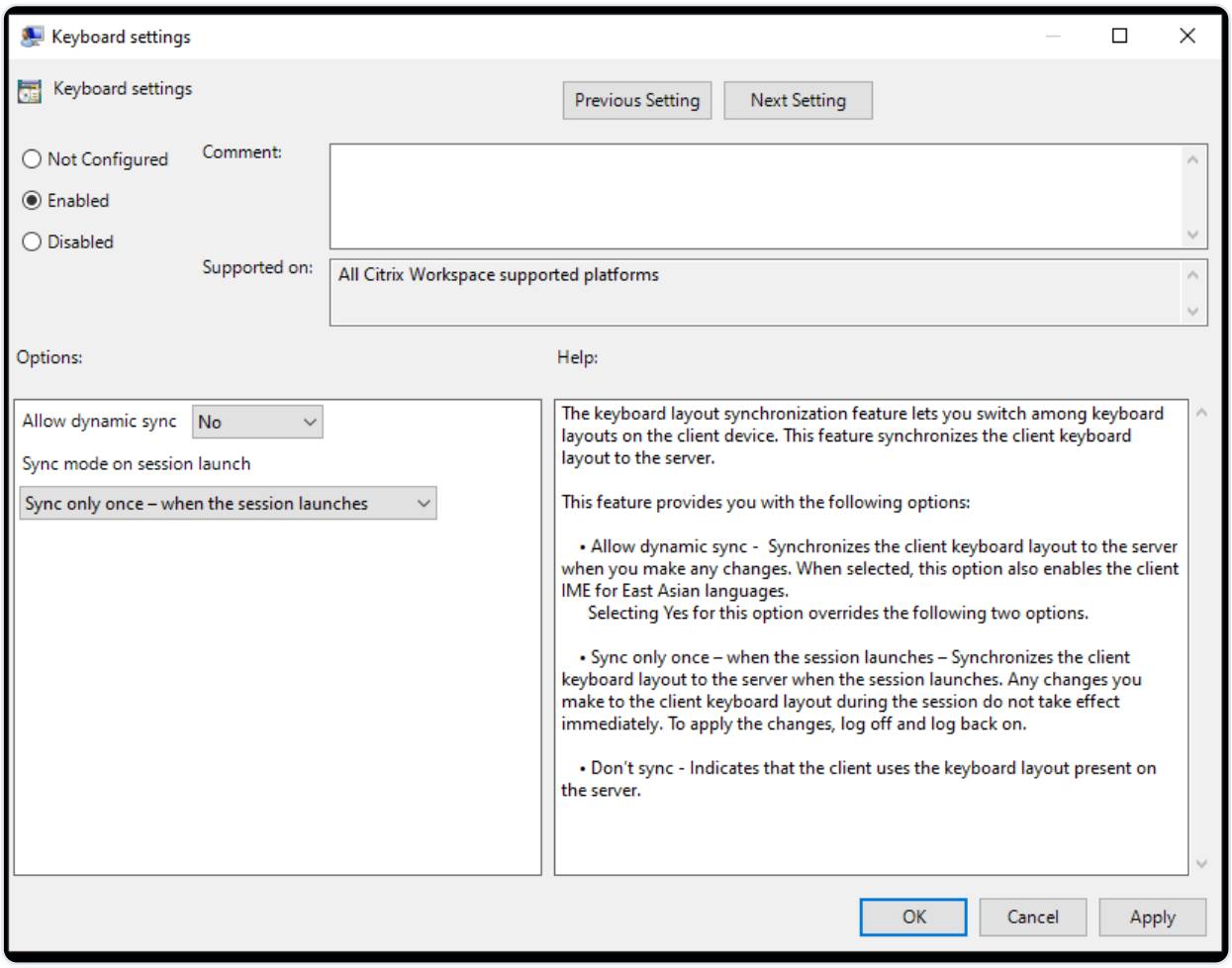
Keyboard layout synchronization enables you to switch among preferred keyboard layouts on the client device. This feature is disabled by default. The keyboard layout synchronization allows the client keyboard layout to automatically synchronize to the virtual apps and desktops session.

To configure keyboard layout synchronization using the GPO administrative template:

> **Note:**
>
> The GPO configuration takes precedence over the StoreFront and the GUI configurations.

1. Open the Citrix Workspace app Group Policy Object administrative template by running gpedit.msc.
2. Under the **Computer Configuration** or **User Configuration** node, go to **Administrative Templates** > **Administrative Templates (ADM)** > **Citrix Components** > **Citrix Workspace** > **User experience**.

3. Select the **Keyboard settings** policy.



4. Select **Enabled** and select one the following options:

   - **Allow dynamic sync** - From the drop-down menu, select **Yes** or **No**. This option synchronizes the client keyboard layout to the server when you change the client keyboard layout. When selected, this option also enables the client IME for East Asian languages.

     Selecting **Yes** for this option overrides the following two options.

   - **Sync mode on session launch** - From the drop-down menu, select one of the following options:

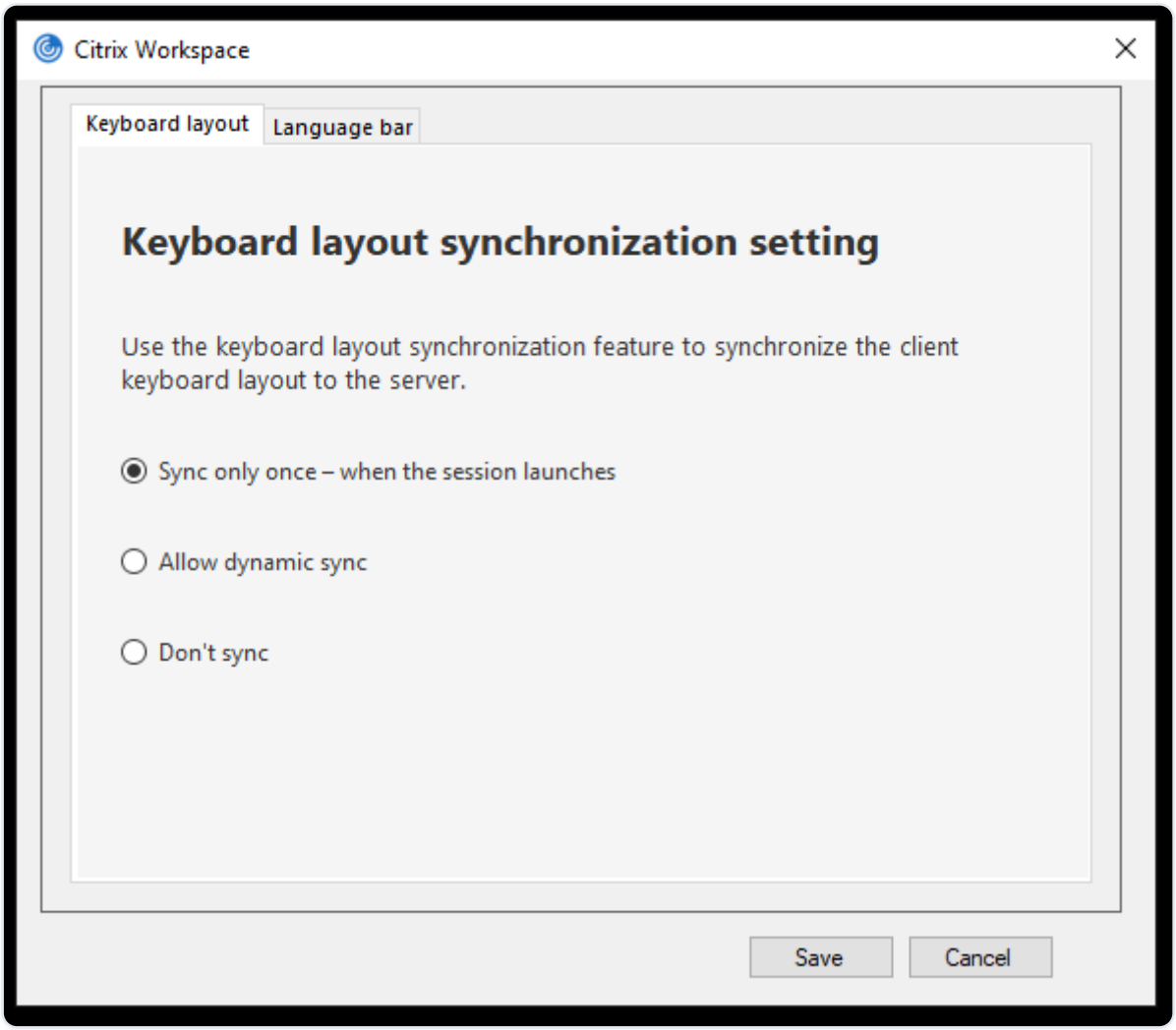
     - **Sync only once - when session launches** - Synchronizes the client keyboard layout to the server when the session launches. Any changes you make to the client keyboard layout during the session do not take effect immediately. To apply the changes, log off and log back on.
     - **Don't sync** - Indicates that the client uses the keyboard layout present on the server.

5. Select **Apply** and **OK**.

To configure keyboard layout synchronization using the graphical user interface:

1. From the Citrix Workspace app icon in the notification area icon, select **Advanced Preferences** > **Keyboard and Language bar**.

   The **Keyboard and Language bar** dialog appears.



2. Select from one of the following options:

   - **Sync only once - when the session launches** - Indicates that the keyboard layout is synced from the VDA only once at the session launch.
   - **Allow dynamic sync** - Indicates that the keyboard layout is synced dynamically to the VDA when the client keyboard is changed in a session.
   - **Don't sync** - Indicates that the client uses the keyboard layout present on the server.

3. Click **Save**.

To configure keyboard layout synchronization using CLI:

Run the following command from the Citrix Workspace app for Windows installation folder.

Typically, the Citrix Workspace app installation folder is at `C:\Program files (x86)\Citrix\ICA Client`.

- To enable: `wfica32:exe /localime:on`
- To disable: `wfica32:exe /localime:off`

Using the client keyboard layout option activates the Client IME (Input Method Editor). If users working in Japanese, Chinese, or Korean prefer to use the Server IME, they must disable the client keyboard layout option by selecting **No**, or running `wfica32:exe /localime:off`. The session reverts to the keyboard layout provided by the remote server when they connect to the next session.

Sometimes, switching the client keyboard layout does not take effect in an active session. To resolve this issue, log off from Citrix Workspace app and login again.

Configure keyboard layout synchronization using the command-line interface

Previously, it was possible to configure keyboard layout synchronization using the GUI or by updating the configuration file only. With the Citrix Workspace app 2309 version, the following commands are introduced to configure keyboard layout synchronization using the command-line-interface:

COMMANDS	DESCRIPTION
`wfica32.exe /kbdsyncmode:once`	Sets keyboard sync mode to "Sync only once".
`wfica32.exe /kbdsyncmode:dynamic`	Sets keyboard sync mode to "Dynamic sync".
`wfica32.exe /kbdsyncmode:no`	Sets keyboard sync mode to "Don't sync".

Run the preceding commands from the Citrix Workspace app for Windows installation folder.

Typically, Citrix Workspace app installation folder is at C:\Program files (x86)\Citrix\ICA Client.

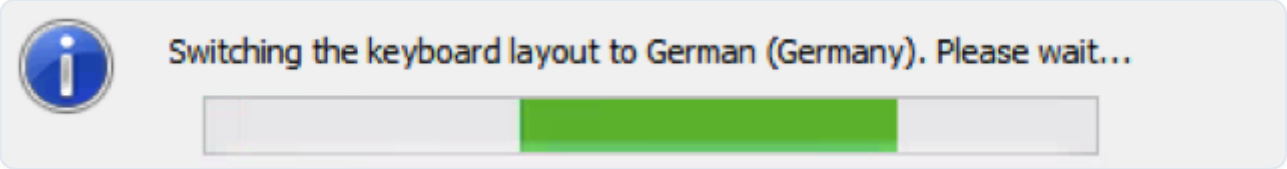
Configuring keyboard sync on Windows VDA

> **Note:**

> The following procedure applies only on Windows server 2016 and later. On Windows Server 2012 R2 and earlier, the keyboard sync feature is enabled by default.

1. Launch the Registry editor and navigate to `HKEY_LOCAL_MACHINE\Software\Citrix\IcaIme`.
2. Create the DWORD entry `DisableKeyboardSync` and set its value to `0`. `1` disables the keyboard layout sync feature.
3. Restart the session for the changes to take effect.

After you enable the keyboard layout on both the VDA and Citrix Workspace app, the following window appears when you switch keyboard layouts.



This window indicates that the session keyboard layout is being switched to the client keyboard layout.

Configuring keyboard sync on Linux VDA

Launch the command prompt and run the following command:

```
/opt/Citrix/VDA/bin/ctxreg update -k "HKEY_LOCAL_MACHINE\System\CurrentControlSet\Control\Citrix\LanguageBar" -v "SyncKeyboardLayout" -d "0x00000001"
```

Restart the VDA for the changes to take effect.

For more information about the keyboard layout synchronization feature on Linux VDA, see Dynamic keyboard layout synchronization.

Hide the keyboard layout switch notification dialog:

The keyboard layout change notification dialog lets you know that the VDA session is switching the keyboard layout. The keyboard layout switch needs approximately two seconds to switch. When you hide the notification dialog, wait for some time before you start typing to avoid incorrect character input.

> **Warning**
>
> Editing the registry incorrectly can cause serious problems that might require you to reinstall your operating system. Citrix can't guarantee that problems resulting from the incorrect use

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

> **Hide the keyboard layout switch notification dialog using the Registry editor:**

1. Launch the Registry editor and navigate to `HKEY_LOCAL_MACHINE\Software\Citrix\IcaIme`.
2. Create a String Value key by name **HideNotificationWindow**.
3. Set the DWORD value to **1**.
4. Click **OK**.
5. Restart the session for the changes to take effect.

Limitations:

- Remote applications which run with elevated privilege (for example, right-click an application icon \> Run as administrator) cannot be synchronized with the client keyboard layout. As a workaround, manually change the keyboard layout on the server side (VDA) or disable UAC.
- If the keyboard layout on the client is changed to an unsupported layout on the server, the synchronization feature of the keyboard layout is disabled for security reasons. An unrecognized keyboard layout is treated as a potential security threat. To restore the keyboard layout synchronization feature, log off and relog in to the session.
- In an RDP session, you cannot change the keyboard layout using `Alt + Shift` shortcuts. As a workaround, use the language bar in the RDP session to switch the keyboard layout.

Language bar

The language bar displays the preferred input language in a session. The language bar appears in a session by default.

> **Note:**

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

> **Configure the language bar using the GPO administrative template:**

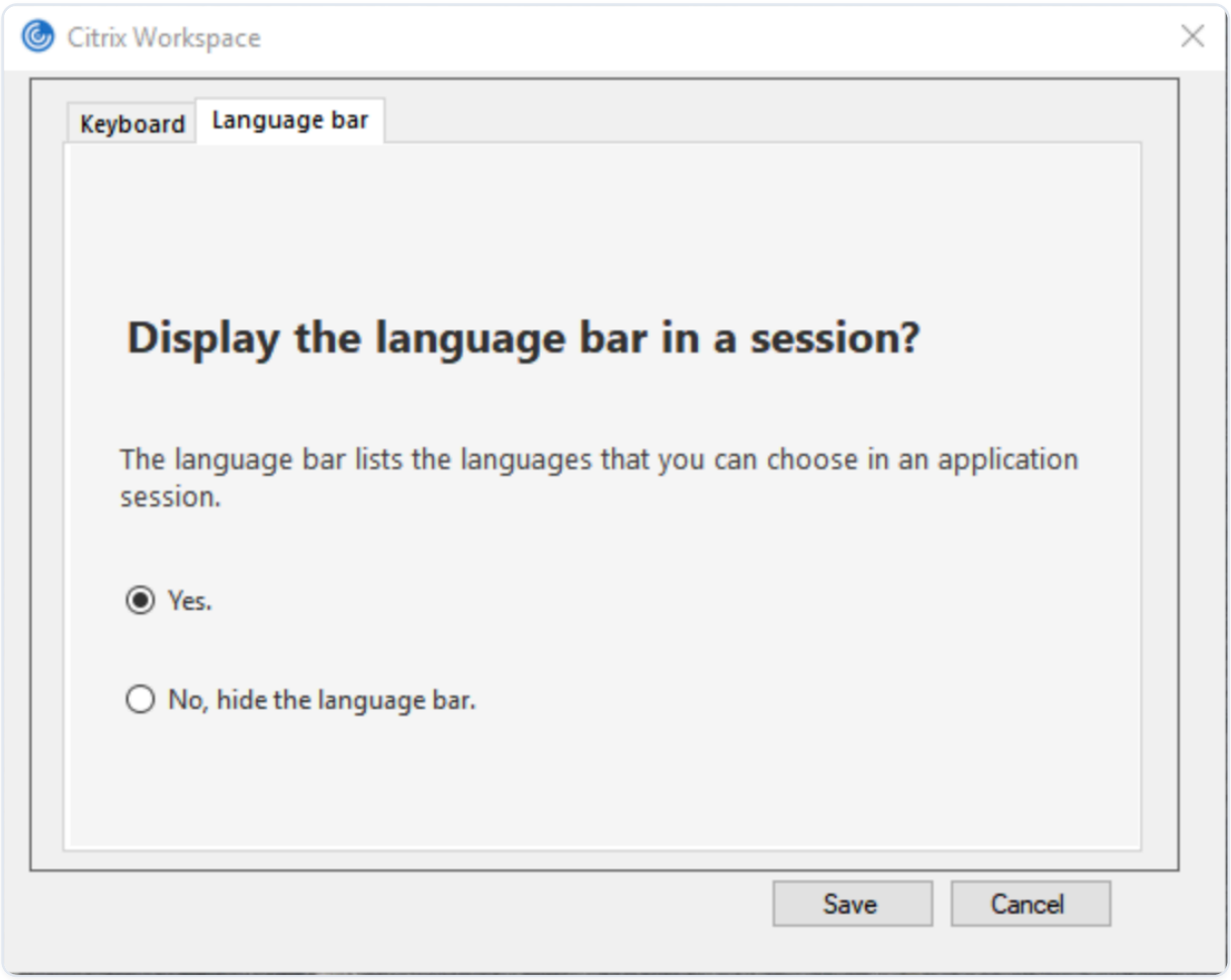
The language bar displays the preferred input language in an application session.

1. Open the Citrix Workspace app Group Policy Object administrative template by running gpedit.msc.
2. Under the **Computer Configuration** or **User Configuration** node, go to **Administrative Templates** > **Administrative Templates (ADM)** > **Citrix Components** > **Citrix Workspace** > **User experience**.
3. Select the **Language bar** policy.
4. Select **Enabled** and select one of the following options:
    - Yes – Indicates that the language bar appears in an application session.
    - No, hide the language bar – Indicates that the language bar is hidden in an application session.
5. Click **Apply** and **OK**.

Configure language bar using the graphical user interface:

1. Right-click the Citrix Workspace app icon from the notification area and select **Advanced Preferences**.
2. Select **Keyboard and Language bar**.
3. Select the **Language bar** tab.
4. Select from one of the following options:
    a. Yes - Indicates that the language bar appears 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.



Note:

- You can change the settings in an active session.
- The remote language bar does not appear in a session if there is only one input language.

Hide the language bar tab from the Advanced Preferences sheet:

You can hide the language bar tab from the **Advanced Preferences** sheet by using the registry.

1. Launch the registry editor.
2. Navigate to `HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\ICA Client\Engine\Configuration\Advanced\Modules\LocalIME`.
3. Create a DWORD value key **ToggleOffLanguageBarFeature**, and set it to **1** to hide the Language bar option from the Advanced Preferences sheet.

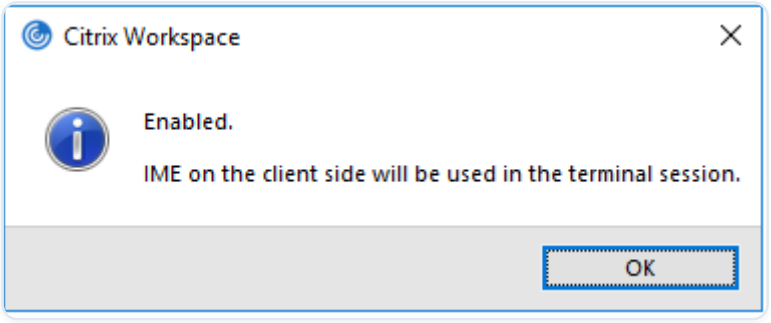
Generic client Input Method Editors (IME)

Note:

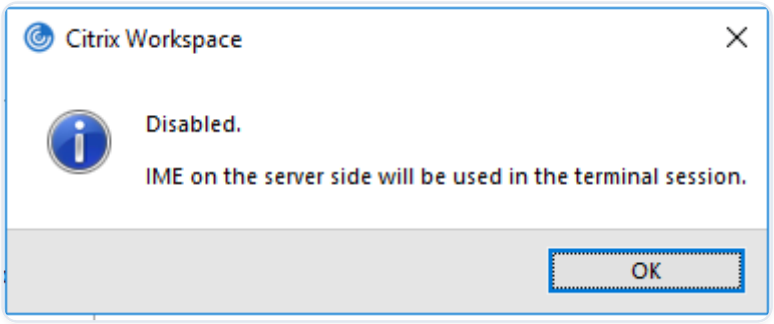
If you're using a Windows 10 Version 2004 operating system, you might face certain technical issues when using the IME feature in a session. Those issues are the result of a third-party limitation. For more information, see the Microsoft Support article.

Configuring generic client IME using the command-line interface:

- To enable generic client IME, run the `wfica32.exe /localime:on` command from the Citrix Workspace app installation folder `C:\Program Files (x86)\Citrix\ICA Client`.



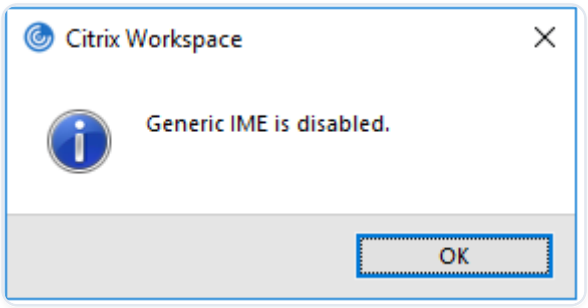
- To disable generic client IME, run the `wfica32.exe /localime:off` command from the Citrix Workspace app installation folder `C:\Program Files (x86)\Citrix\ICA Client`.



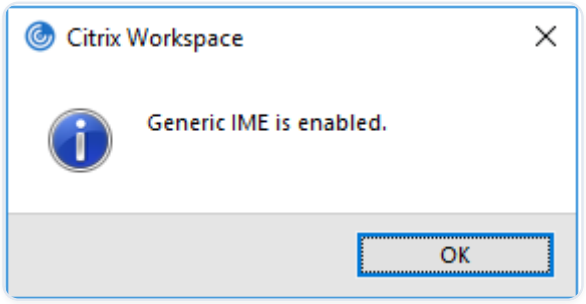
Note:

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

- 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 the layout synchronization setting is set as **Off**, toggling does not enable generic client IME.

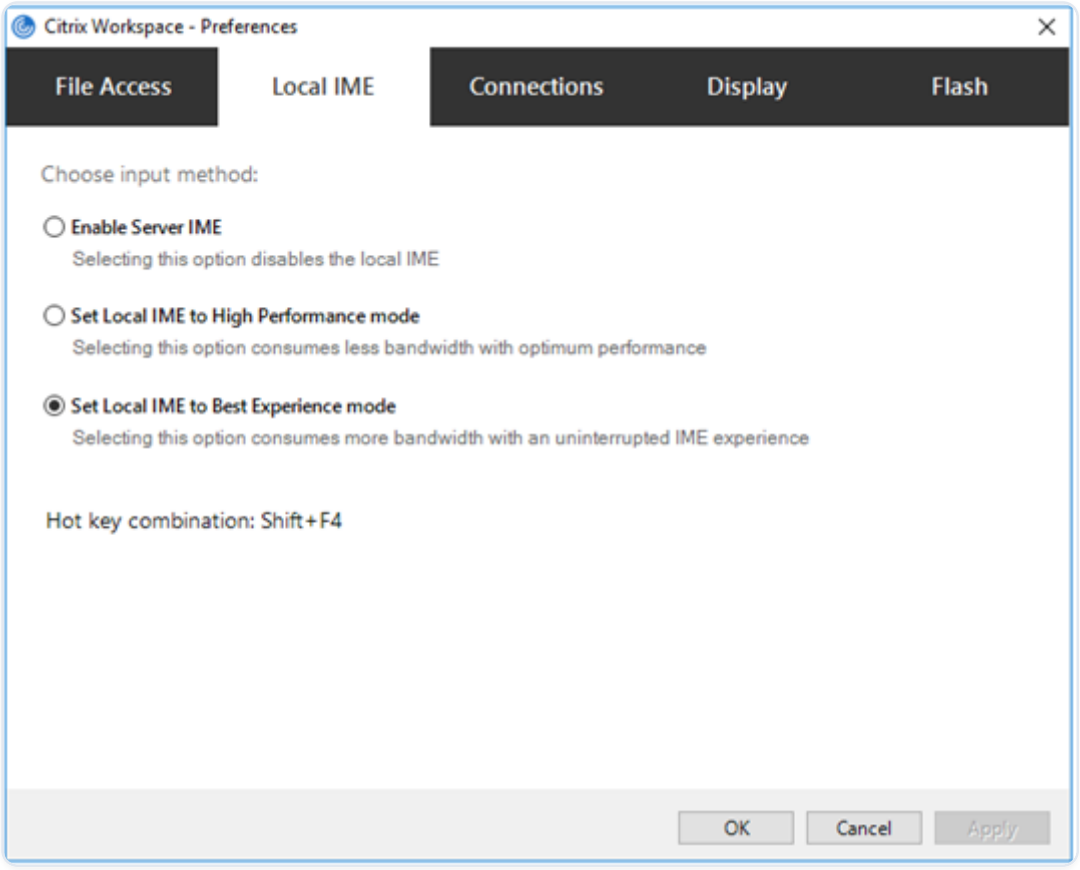
Configure generic client IME using the graphical user interface:

Generic client IME requires VDA Version 7.13 or later.

The 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. Right-click the Citrix Workspace app icon in the notification area and select **Connection Center**.
2. Select **Preferences** and **Local IME**.



The following options are available to support different IME modes:

1. **Enable Server IME** – Disables local IME and only the languages set on the server can be used.
2. **Set Local IME to High Performance mode** – Uses local IME with limited bandwidth. This option restricts the candidate window functionality.
3. **Set Local IME to Best Experience mode** – Uses local IME with best user experience. This option consumes high bandwidth. By default, this option is selected when generic client IME is enabled.

The changes are applied only for the current session.

Enabling hotkey configuration using a registry editor:

When generic client IME is enabled, you can use the **Shift+F4** hotkeys to select different IME modes. The different options for IME modes appear in the top-right corner of the session.

By default, the hotkey for generic client IME is disabled.

In the registry editor, navigate to `HKEY_CURRENT_USER\SOFTWARE\Citrix\ICA Client\Engine\Lockdown Profiles\All Regions\Lockdown\Client Engine\Hot Key`.

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

You can use the **Shift+F4** hotkeys to select different IME modes in a session.

The different options for IME modes appear in the top-right corner of the session while switching using these hotkey combinations.



Limitations:

- Generic client IME does not support UWP (Universal Windows Platform) apps such as Search UI, and the Edge browser of the Windows 10 operating system. As a workaround, use the server IME instead.
- Generic client IME is not supported on Internet Explorer Version 11 in **Protected Mode**. As a workaround, you can disable Protected Mode by using **Internet Options**. To disable, click **Security** and clear **Enable Protected Mode**.

Synchronize multiple keyboards at session start

Previously, only the active keyboard on the client was synchronized with VDA after the session started in full-screen mode. In this scenario, if you configured **Sync only once - when session launches** on your Citrix Workspace app, and you had to change to a different keyboard, you have to manually install the keyboard on your remote desktop. Similarly, if you configured **Allow dynamic sync** on your Citrix Workspace app, you have to move to windowed mode, change the keyboard on your client, and then move back to full-screen mode.

Starting with the 2311.1 release, all available keyboards on the client are synchronized with VDA after the session starts in full-screen mode. You can select the required keyboard from the list of installed or available keyboards on the client after the session starts in full-screen mode.

The **Synchronize multiple keyboards at session start** feature is enabled by default on VDA, and disabled by default on the Citrix Workspace app.

Prerequisites

On Citrix Workspace app for Windows:

Enable **Sync only once - when the session launches** keyboard layout setting. For more information, see Keyboard layout documentation.

On VDA:

Enable the following VDA policies:

- Unicode Keyboard Layout Mapping. For more information, see Enable Unicode keyboard layout mapping or Keyboard and Input Method Editor (IME)
- Client keyboard layout synchronization and IME improvement. For more information, see Keyboard and Input Method Editor (IME)

Citrix Workspace app configuration:

This feature is applicable only on virtual desktops. This feature is disabled by default. To enable this feature, do the following:

1. Navigate to the section of the **All_Regions.ini** file.
2. Add a Boolean registry key `SyncKbdLayoutList to HKEY_CURRENT_USER\SOFTWARE\Citrix\Ica Client\Engine\Lockdown Profiles\All Regions\Lockdown\Virtual Channels\Keyboard`.
3. Set the value to 1.

VDA configuration:

The feature **Synchronize multiple keyboards at session start** is enabled by default on VDA. To disable this feature, update the VDA registry as follows:

1. Open the Registry editor and navigate to `HKEY_LOCAL_MACHINE\Software\Citrix\IcaIme`.
2. Create the DWORD entry `DisableKbdLayoutList` and set its value to 0. Setting the value to 1, disables the **Synchronize multiple keyboards at session start** feature.
3. Restart the session for the changes to take effect.

Printing

Printer

To override the printer settings on the user device

1. From the **Print** menu available from an application on the user device, choose **Properties**.
2. On the **Client Settings** tab, click Advanced Optimizations and modify the Image Compression and Image and Font Caching options.

On-screen keyboard control

To enable touch-enabled access to virtual applications and desktops from Windows tablets, Citrix Workspace app automatically displays the on-screen keyboard when:

- you activate a text entry field and
- when the device is in tent or tablet mode.

On some devices and in some circumstances, Citrix Workspace app can't accurately detect the mode of the device. The on-screen keyboard might also appear when you don't want it to.

To suppress the on-screen keyboard from appearing when using a convertible device:

- create a REG_DWORD value DisableKeyboardPopup in `HKEY\_CURRENT\_USER\ \SOFTWARE\\Citrix\\ICA Client\\Engine\\Configuration\\Advanced\\Modules\ \MobileReceiver` and
- set the value to 1.

> **Note:**

> On a x64 machine, create the value in HKEY_LOCAL_MACHINE\\SOFTWARE\ \Wow6432Node\\Citrix\\ICA Client\\Engine\\Configuration\\Advanced\\Modules\ \MobileReceiver.

> The keys can be set to the following 3 different modes:

- **Automatic**: AlwaysKeyboardPopup = 0; DisableKeyboardPopup = 0
- **Always popup** (on-screen keyboard): AlwaysKeyboardPopup = 1; DisableKeyboardPopup = 0
- **Never popup** (on-screen keyboard): AlwaysKeyboardPopup = 0; DisableKeyboardPopup = 1

PDF printing

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

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

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

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

Prerequisites:

- Citrix Virtual Apps and Desktops™ Version 7 1808 or later.
- At least one PDF viewer must be installed on your computer.

To enable PDF printing:

1. On the Delivery Controller, use the Citrix Studio, to select the **Policy** node in the left pane. You can either create a policy or edit an existing policy.
2. Set the **Auto-create PDF Universal Printer** policy to Enabled.

Restart the Citrix Workspace app session for the changes to take effect.

Limitation:

- PDF viewing and printing aren't supported on the Microsoft Edge browser.

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 supports Windows Continuum, including dynamic change of modes.

For touch-enabled devices, the Windows 10 VDA starts in tablet mode when there's no keyboard or mouse attached. It starts in desktop mode when either a keyboard or a mouse or both are attached. Detaching or attaching the keyboard on any client device or the screen on a 2-in-1 device like a Surface Pro toggles between tablet and desktop modes. For more information, see Tablet mode for touchscreen devices in Citrix Virtual Apps and Desktops documentation.

On a touch-enabled client device, the Windows 10 VDA detects the presence of a keyboard or mouse when you connect or reconnect to a session. It also detects when you attach or detach a keyboard or mouse during the session. This feature is enabled by default on the VDA. To disable the feature, modify the **Tablet mode toggle** policy using Citrix Studio.

Tablet mode offers a user interface that is better suited to touchscreens:

- Slightly larger buttons.
- The **Start** screen and all the apps you start open in a full screen.
- The taskbar includes a Back button.
- Icons are removed from the taskbar.

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

> **Note:**
>
> Workspace for web doesn't support the Windows Continuum feature.

USB

USB support

USB support enables you to interact with a wide range of USB devices when connected to a Citrix Virtual Apps and Desktops™ and Citrix DaaS. You can plug USB devices into their computers and the devices are remote to their virtual desktop. USB devices available for remoting include flash drives, smartphones, PDAs, printers, scanners, MP3 players, security devices, and tablets. Desktop Viewer users can control whether USB devices are available on the Citrix Virtual Apps and Desktops and Citrix DaaS using a preference in the toolbar.

Isochronous features in USB devices, such as webcams, microphones, speakers, and headsets are supported in typical low latency or high-speed LAN environments. Such environment allows these devices to interact with packages, like Microsoft Office Communicator and Skype.

The following types of device are supported directly in a virtual apps and desktops session, and so does not use USB support:

- Keyboards

- Mice
- Smart cards

Specialist USB devices (for example, Bloomberg keyboards and 3-D mice) can be configured to use USB support. For information on configuring Bloomberg keyboards, see Configure Bloomberg keyboards.

For information on configuring policy rules for other specialist USB devices, see Knowledge Center article CTX122615.

By default, certain types of USB devices are not supported for remoting through Citrix Virtual Apps and Desktops and Citrix DaaS. For example, a user might have a NIC attached to the system board by internal USB. Remoting this device would not be appropriate. The following types of USB device are not supported by default in a virtual apps and desktops session:

- Bluetooth dongles
- Integrated NIC
- USB hubs
- USB graphics adapters

USB devices connected to a hub can be remote, but the hub itself cannot be remote.

The following types of USB device are not supported by default for use in a virtual apps session:

- Bluetooth dongles
- Integrated NIC
- USB hubs
- USB graphics adapters
- Audio devices
- Mass storage devices

How USB support works:

When a user plugs in a USB device, it is checked against the USB policy, and, if allowed, remoted to the virtual desktop. If the default policy denies a device, it is available only to the local desktop.

When a user plugs in a USB device, a notification appears to inform the user about a new device. The user can select which USB devices must be remoted to the virtual desktop each time they

connect. Alternatively, the user can configure USB support so that all USB devices plugged in both before and/or during a session is automatically remoted to the virtual desktop that is in focus.

USB device classes allowed by default

Default USB policy rules allow different classes of USB device.

Although they are on this list, some classes are only available for remoting in virtual apps and desktops sessions after additional configuration. Such USB device classes are as follows.

- **Audio (Class 01)**- Includes audio input devices (microphones), audio output devices, and MIDI controllers. Modern audio devices generally use isochronous transfers that XenDesktop® 4 or later supports. Audio (Class01) is not applicable to virtual apps because these devices are not available for remoting in virtual apps using USB support.

> **Note:**
>
> Some specialty devices (for example, VOIP phones) require additional configuration.

- **Physical Interface Devices (Class 05)**- These devices are similar to Human Interface Devices (HIDs), but generally provide "real-time" input or feedback and include force feedback joysticks, motion platforms, and force feedback endoskeletons.
- **Still Imaging (Class 06)**- Includes digital cameras and scanners. Digital cameras often support the still imaging class which uses the Picture Transfer Protocol (PTP) or Media Transfer Protocol (MTP) to transfer images to a computer or other peripheral. Cameras might also appear as mass storage devices. It might be also possible to configure a camera to use either class, through the setup menus provided by the camera itself.

> **Note:**
>
> If a camera appears as a mass storage device, client drive mapping is used and USB support is not required.

- **Printers (Class 07)**- In general most printers are included in this class, although some use vendor-specific protocols (class ff). Multi-function printers might have an internal hub or be composite devices. In both cases the printing element generally uses the Printers class and the scanning or fax element uses another class; for example, Still Imaging.

Printers normally work appropriately without USB support.

> **Note**
>
> This class of device (in particular printers with scanning functions) requires additional configuration.

- **Mass Storage (Class 08)**- The most common mass storage devices are USB flash drives; others include USB-attached hard drives, CD/DVD drives, and SD/MMC card readers. There are a wide variety of devices with internal storage that also present a mass storage interface; these include media players, digital cameras, and mobile phones. Mass Storage (Class 08) is not applicable to virtual apps because these devices are not available for remoting in 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 cover devices that are used to manipulate video or video-related material. Devices, such as webcams, digital camcorders, analog video converters, some television tuners, and some digital cameras that support video streaming.

> **Important**
>
> Most video streaming devices use isochronous transfers that XenDesktop 4 or later supports. Some video devices (for example webcams with motion detection) require additional configuration.

- **Personal Healthcare (Class 0f)**- These devices include personal healthcare devices such as blood pressure sensors, heart rate monitors, pedometers, pill monitors, and spirometry.
- **Application and Vendor Specific (Classes fe and ff)**- Many devices use vendor-specific protocols or protocols not standardized by the USB consortium, and such devices usually appear as vendor-specific (class ff).

USB devices classes denied by default

Default USB policy rules don't allow the following different classes of USB device:

- Communications and CDC Control (Classes 02 and 0a). The default USB policy doesn't allow these devices, because one of the devices might be providing the connection to the virtual desktop itself.
- Human Interface Devices (Class 03). Includes a wide variety of both input and output devices. Typical Human Interface Devices (HIDs) are keyboards, mice, pointing devices, graphic tablets, sensors, game controllers, buttons, and control functions.

  Subclass 01 is known as the "boot interface" class and is used for keyboards and mice.

  The default USB policy doesn't allow USB keyboards (class 03, subclass 01, protocol 1), or USB mice (class 03, subclass 01, protocol 2). The reason is most keyboards and mice are handled appropriately without USB support. Also, it is normally necessary to use these devices locally as well remotely when you connect to a virtual desktop.
- USB Hubs (Class 09). USB hubs allow extra devices to be connected to the local computer. It is not necessary to access these devices remotely.
- Smart Card (Class 0b). Smart card readers include contactless and contact smart card readers, and also USB tokens with an embedded smart card-equivalent chip.

  Smart card readers are accessed using smart card remoting and do not require USB support.
- Wireless Controller (Class e0). Some of these devices might be providing critical network access, or connecting critical peripherals, such as Bluetooth keyboards or mice.

  The default USB policy does not allow these devices. However, there might be particular devices to which it is appropriate to provide access using USB support.
- **Miscellaneous network devices (Class ef, subclass 04)**- Some of these devices might be providing critical network access. The default USB policy does not allow these devices. However, there might be particular devices to which it is appropriate to provide access using USB support.

Update the list of USB devices available for remoting

Edit the Citrix Workspace for Windows template file to update the range of USB devices available for remoting to desktops. The update allows you to change the Citrix Workspace for Windows using Group Policy. The file is in the following installed folder:

`\C:\Program Files\Citrix\ICA Client\Configuration\en`

Alternatively, you can edit the registry on each user device, adding the following registry key:

HKEY_LOCAL_MACHINE\\SOFTWARE\\Policies\\Citrix\\ICA Client\\GenericUSB Type=String Name="DeviceRules" Value=

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

> The product default rules are stored in:

HKEY_LOCAL_MACHINE\\SOFTWARE\\Citrix\\ICA Client\\GenericUSB Type=MultiSz Name="DeviceRules" Value=

Do not edit the product default rules.

For more information about USB devices policy settings, see USB devices policy settings in Citrix Virtual Apps and Desktops documentation.

Composite USB device redirection

USB 2.1 and later supports the notion of USB composite devices where multiple child devices share a single connection with the same USB bus. Such devices employ a single configuration space and shared bus connection where a unique interface number 00-ff is used to identify each child device. Such devices are also not the same as a USB hub which provides a new USB bus origin for other independently addressed USB devices for connection.

Composite devices found on the client endpoint can be forwarded to the virtual host as either:

- a single composite USB device, or

- a set of independent child devices (split devices)

When a composite USB device is forwarded, the entire device becomes unavailable to the endpoint. Forwarding also blocks the local usage of the device for all applications on the endpoint, including the Citrix Workspace client needed for an optimized HDX remote experience.

Consider a USB headset device with both audio device and HID button for mute and volume control. If the entire device is forwarded using a generic USB channel, the device becomes unavailable for redirection over the optimized HDX™ audio channel. However, you can achieve the best experience when the audio is sent through the optimized HDX audio channel unlike the audio sent using host-side audio drivers through generic USB remoting. The behavior is because of the noisy nature of the USB audio protocols.

You also notice issues when the system keyboard or pointing device are part of a composite device with other integrated features required for the remote session support. When a complete composite device is forwarded, the system keyboard or mouse becomes inoperable at the endpoint, except within the remote desktop session or application.

To resolve these issues, Citrix recommends that you split the composite device and forward only the child interfaces that use a generic USB channel. Such mechanism ensures that the other child devices are available for use by applications on the client endpoint, including, the Citrix Workspace app that provides optimized HDX experiences, while allowing only the required devices to be forwarded and available to the remote session.

Device Rules:

As with regular USB devices, device rules set in the policy or client Citrix Workspace app configuration on the end point select the composite devices for forwarding. Citrix Workspace app uses these rules to decide which USB devices to allow or prevent from forwarding to the remote session.

Each rule consists of an action keyword (Allow, Connect, or Deny), a colon (**:**), and zero or more filter parameters that match actual devices at the endpoints USB subsystem. These filter parameters correspond to the USB device descriptor metadata used by every USB device to identify itself.

Device rules are clear text with each rule on a single line and an optional comment after a # character. Rules are matched top down (descending priority order). The first rule that matches the device or child interface is applied. Subsequent rules that select the same device or interface are ignored.

Sample device rules:

- ALLOW: vid=046D pid=0102 # Allow a specific device by vid/pid
- ALLOW: vid=0505 class=03 subclass=01 # Allow any pid for vendor 0505 when subclass=01
- DENY: vid=0850 pid=040C # Deny a specific device (incl all child devices)
- DENY: class=03 subclass=01 prot=01 # Deny any device that matches all filters
- CONNECT: vid=0911 pid=0C1C # Allow and auto-connect a specific device
- ALLOW: vid=0286 pid=0101 split=01 # Split this device and allow all interfaces
- ALLOW: vid=1050 pid=0407 split=01 intf=00,01 # Split and allow only 2 interfaces
- CONNECT: vid=1050 pid=0407 split=01 intf=02 # Split and auto-connect interface 2
- DENY: vid=1050 pid=0407 split=1 intf=03 # Prevent interface 03 from being remoted

You can use any of the following filter parameters to apply rules to the encountered devices:

FILTER PARAMETER	DESCRIPTION
vid=xxxx	USB device vendor ID (four-digit hexadecimal code)
pid=xxxx	USB device product ID (four-digit hexadecimal code)
rel=xxxx	USB device release ID (four-digit hexadecimal code)
class=xx	USB device class code (two-digit hexadecimal code)
subclass=xx	USB device subclass code (two-digit hexadecimal code)
prot=xx	USB device protocol code (two-digit hexadecimal code)
split=1 (or split=0)	Select a composite device to be split (or non-split)
intf=xx[,xx,xx,...]	Selects a specific set of child interfaces of a composite device (comma-separated list of two-digit hexadecimal codes)

The first six parameters select the USB devices for which the rule must be applied. If any parameter is not specified, the rule matches a device with ANY value for that parameter.

The USB Implementors Forum maintains a list of defined class, subclass, and protocol values in Defined Class Codes. USB-IF also maintains a list of registered vendor IDs. You can check the vendor, product, release, and interface IDs of a specific device directly in the Windows device manager or using a free tool like UsbTreeView.

When present, the last two parameters apply only to USB composite devices. The split parameter determines if a composite device must be forwarded as split devices or as a single composite device.

- *Split=1* indicates that the selected child interfaces of a composite device must be forwarded as split devices.
- *Split=0* indicates that the composite device must not be split.

> **Note:**
>
> If the split parameter is omitted, *Split=0* is assumed.

> The *intf* parameter selects the specific child interfaces of the composite device to which the action must be applied. If omitted, the action applies to all interfaces of the composite device.

Consider a composite USB headset device with three interfaces:

- Interface 0 - Audio class device endpoints
- Interface 3 - HID class device endpoints (volume and mute buttons)
- Interface 5 - Management/update interface

The suggested rules for this type of device are:

- CONNECT: vid=047F pid=C039 split=1 intf=03 # Allow and auto-connect HID device
- DENY: vid=047F pid=C039 split=1 intf=00 # Deny audio end points
- ALLOW: vid=047F pid=C039 split=1 intf=05 # Allow mgmt intf but don’t auto-connect

Enable Device Rules policy:

Citrix Workspace app for Windows includes a set of default device rules that filters certain undesirable classes of devices and allow one that customers often encounter.

You can check these default device rules in the system registry at either:

- `HKEY_LOCAL_MACHINE\Software\Citrix\ICA Client\GenericUSB` (32-bit Windows) or
- `HKEY_LOCAL_MACHINE\Software\WOW6432Node\Citrix\ICA Client\GenericUSB` (64-bit Windows), in the multistring value named **DeviceRules**.

However, in the Citrix Workspace app for Window, you can apply **USB Device Rules** policy to overwrite these default rules.

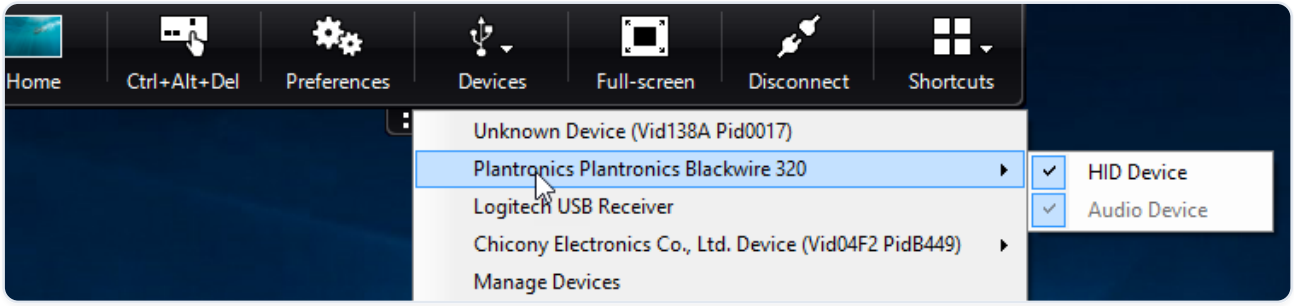
To enable device rules policy for Citrix Workspace app for Windows:

1. Open the Citrix Workspace app Group Policy Object administrative template by running gpedit.msc.
2. Under the **User Configuration** node, go to **Administrative Templates** \> **Citrix Components** \> **Citrix Workspace** \> **Remoting client devices** \> **Generic USB Remoting**.
3. Select the **USB Device Rules** policy.
4. Select **Enabled**.
5. In the **USB Device Rules** text box, paste (or edit directly) the USB device rules to be deployed.
6. Click **Apply** and **OK**.

Citrix recommends preserving the default rules shipped with the client when creating this policy by copying the original rules and inserting new rules to alter the behavior as desired.

Connecting USB devices:

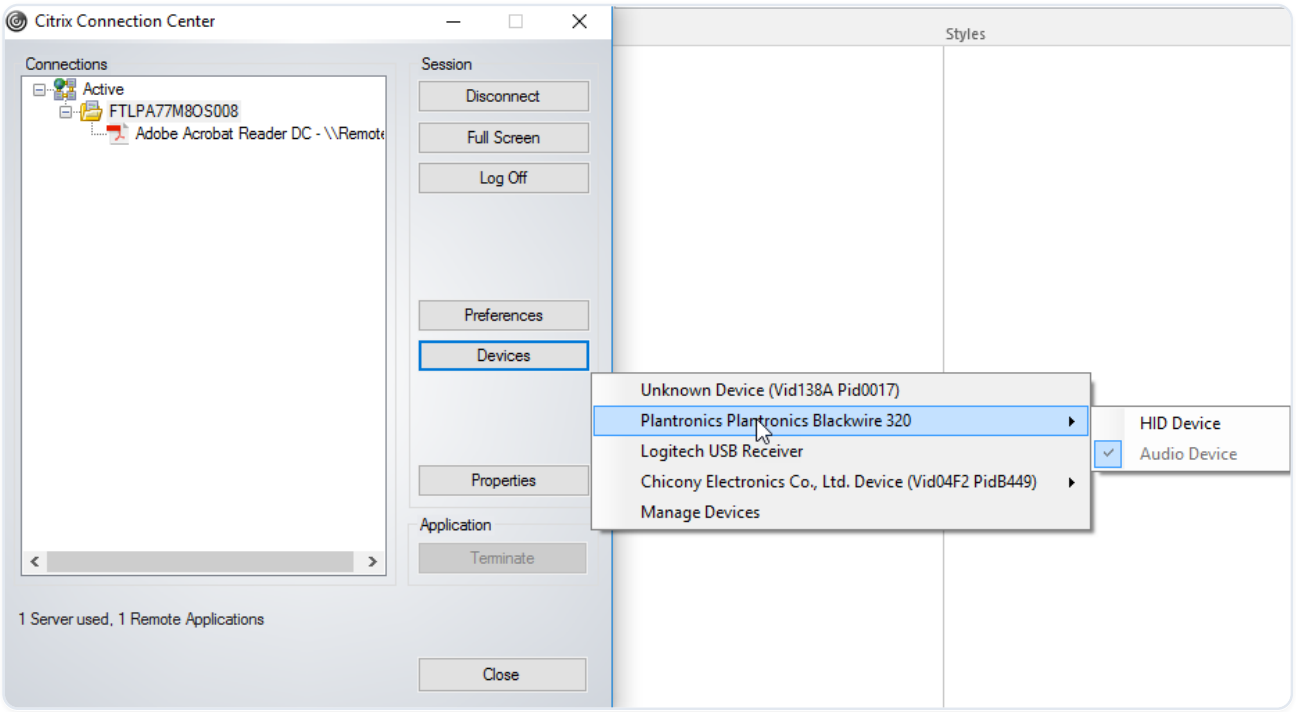
In a desktop session, split USB devices are displayed in the Desktop Viewer under **Devices**. Also, you can view split USB devices from **Preferences** \> **Devices**.



> **Note:**
>
> CONNECT keyword enables automatic connection of a USB device. However, if the CONNECT keyword is not used when you split a composite USB device for generic USB

redirection, you must manually select the device from the Desktop Viewer or Connection Center to connect an allowed device.

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



To automatically connect an interface:

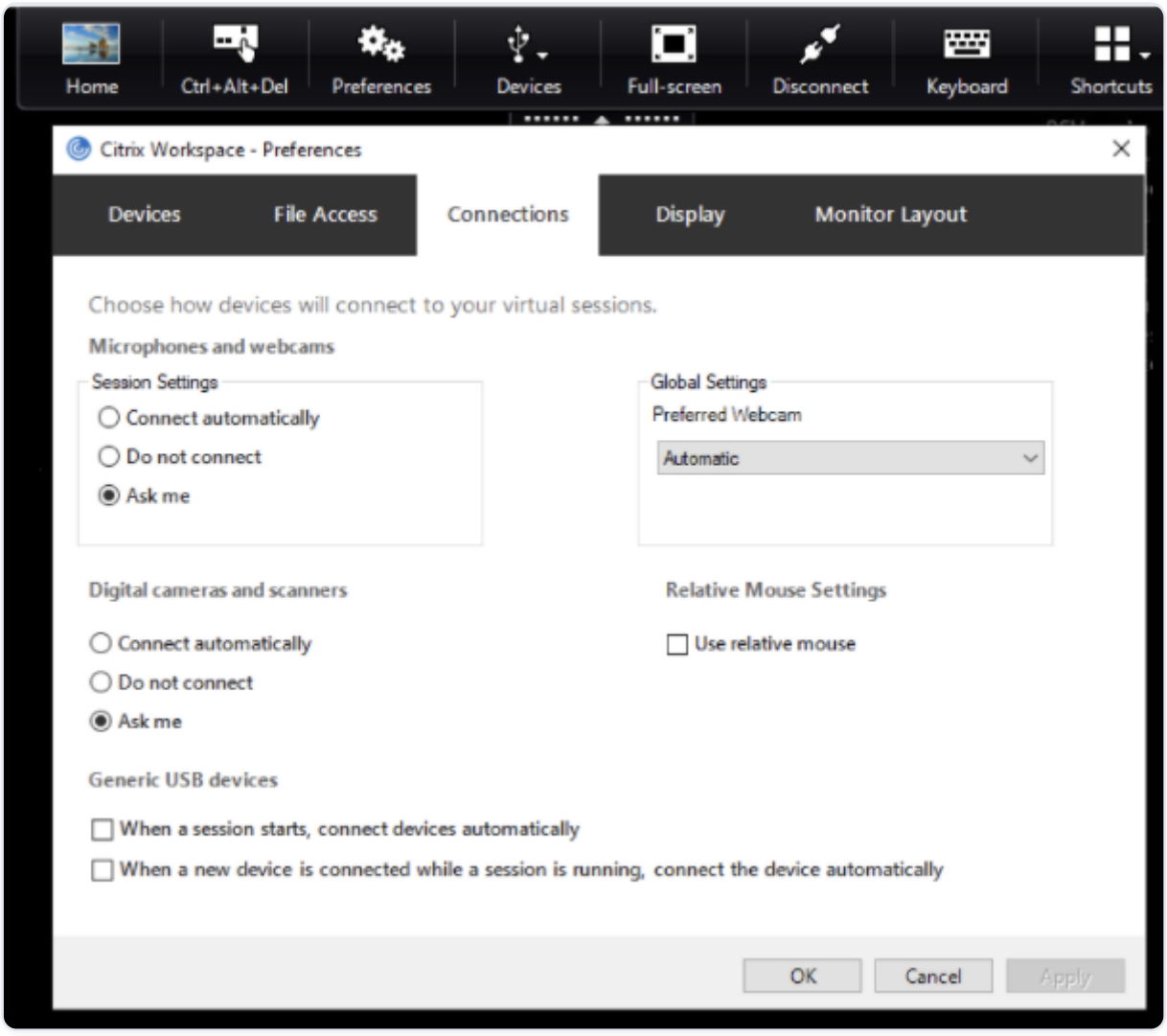
The CONNECT keyword introduced in Citrix Workspace app for Windows 2109 allows for automatic redirection of USB devices. The CONNECT rule can replace the ALLOW rule if the administrator allows the device or selected interfaces to automatically connect in the session.

1. Open the Citrix Workspace app Group Policy Object administrative template by running gpedit.msc.
2. Under the **User Configuration** node, go to **Administrative Templates** \> **Citrix Components** \> **Citrix Workspace** \> **Remoting client devices** \> **Generic USB Remoting**.
3. Select the **USB Device Rules** policy.
4. Select **Enabled**.
5. In the **USB Device Rules** text box, add the USB device that you want to auto connect.

   For example, CONNECT: vid=047F pid=C039 split=01 intf=00,03 – allows for splitting a composite device and auto connection of interfaces 00 and 03 interface and restriction other interfaces of that device.
6. Click **Apply** and **OK** to save the policy.

Changing USB device auto-connection preferences:

Citrix Workspace app automatically connects USB devices tagged with CONNECT action based on the preferences set for the current desktop resource. You can change the preferences in the **Desktop viewer** toolbar as shown in the following image.



The two check boxes at the bottom of the pane controls if the devices must connect automatically or wait for manual connection in the session. These settings are not enabled by default. You can change the preferences if generic USB devices must be connected automatically.

Alternatively, an administrator can override the user preferences by deploying the corresponding policies from Citrix Workspace app Group Policy Object administrative template. Both machine and user policies can be found under **Administrative Templates** \> **Citrix Components** \> **Citrix Workspace** \> **Remoting client devices** \> **Generic USB Remoting**. The corresponding policies are labeled as Existing USB Devices and New USB Devices respectively.

Change split device default setting:

By default, the Citrix Workspace app for Windows only splits composite devices that are explicitly tagged as *Split=1* in the device rules. However, it is possible to change the default disposition to split all composite devices that are not otherwise tagged with *Split=0* in a matching device rule.

1. Open the Citrix Workspace app Group Policy Object administrative template by running gpedit.msc.
2. Under the **User Configuration** node, go to **Administrative Templates** \> **Citrix Components** \> **Citrix Workspace** \> **Remoting client devices** \> **Generic USB Remoting**.
3. Select the **SplitDevices** policy.
4. Select **Enabled**.
5. Click **Apply** and **OK** to save the policy.

> **Note:**
>
> Citrix recommends using explicit device rules to identify specific devices or interfaces that need to be split instead of changing the default. This setting will be deprecated in a future release.

> **Limitation:**

- Citrix recommends that you do not split interfaces for a webcam. As a workaround, redirect the device to a single device using Generic USB redirection. For a better performance, use the optimized virtual channel.
- Sometimes, USB composite devices might not be split automatically even though a correct device redirection rule is set to split the device. The issue occurs because the device is in low power mode. In these instances, the child device that enters low power mode might not be present in the device list. You can use one of the following workarounds to overcome this issue:
  - Disconnect the session, insert the USB device, and reconnect to the session.
  - Unplug the USB device and plug it back in. This action results in the device moving out of low power mode.

Bloomberg keyboards

Citrix Workspace app supports the use of Bloomberg keyboard in a virtual apps and desktops session. The required components are installed with the plug-in. You can enable the Bloomberg keyboard feature when installing Citrix Workspace app for Windows or by using the Registry editor.

Bloomberg keyboards provide other functionality when compared to standard keyboards that allow the user to access financial market data and perform trades.

The Bloomberg keyboard consists of multiple USB devices built into one physical shell:

- the keyboard
- a fingerprint reader
- an audio device
- a USB hub to connect all of these devices to the system
- HID buttons, for example, Mute, Vol Up, and Vol Down for the audio device

In addition to the normal functionality of these devices, the audio device includes support for some keys, control of the keyboard, and keyboard LEDs.

To use the specialized functionality inside a session, you must redirect the audio device as a USB device. This redirect makes the audio device available to the session, but prevents the audio device from being used locally. In addition, the specialized functionality can only be used with one session and cannot be shared between multiple sessions.

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

Configuring Bloomberg keyboard 5:

Starting from Citrix Workspace app for Windows 2109 version, a new CONNECT keyword is introduced to allow automatic connection of USB devices at session startup and device insertion. The CONNECT keyword can be used to replace the ALLOW keyword when the user wants a USB device or interface to connect automatically.

> **Note:**
>
> With the introduction of Device redirection rules version 2 in Studio in Citrix Virtual Apps and Desktops 2212 version, it isn't required to configure the Bloomberg 5 keyboard through client-side group policies in Citrix Workspace app for Windows. For more details, see Client USB device redirection rules (Version 2) in Citrix Virtual Apps and Desktops documentation.

> For versions prior to Citrix Workspace app for Windows version 2212, the following example shows how to use the CONNECT keyword:

1. Open the Citrix Workspace app Group Policy Object administrative template by running gpedit.msc.
2. Under the **Computer Configuration** node, go to **Administrative Templates** \> **Citrix Components** \> **Citrix Workspace** \> **Remoting client devices** \> **Generic USB Remoting**.
3. Select the **SplitDevices** policy.
4. Select **Enabled**.
5. In the **USB Device Rules** text box, add the following rules if it doesn't exist.
    - CONNECT: vid=1188 pid=A101 # Bloomberg 5 Biometric module
    - DENY: vid=1188 pid=A001 split=01 intf=00 # Bloomberg 5 Primary keyboard
    - CONNECT: vid=1188 pid=A001 split=01 intf=01 # Bloomberg 5 Keyboard HID
    - DENY: vid=1188 pid=A301 split=01 intf=02 # Bloomberg 5 Keyboard Audio Channel
    - CONNECT: vid=1188 pid=A301 split=01 intf=00,01 # Bloomberg 5 Keyboard Audio HID

    > **Note:**
    >
    > New lines or semicolon can be used to separate rules which allows to read either single line or multi-line registry values.

6. Click **Apply** and **OK** to save the policy.
7. In the **Preferences** window, select the **Connections** tab, and select one or both check boxes to the connect devices automatically. The **Preferences** window is accessible from the Desktop Toolbar or Connection Manager.

This procedure makes the Bloomberg keyboard 5 ready for use. The DENY rules that are mentioned in the steps enforce the redirection of the primary keyboard and audio channel over an optimized channel but not over Generic USB. The CONNECT rules enable automatic redirection of the fingerprint module, special keys on the keyboard, and keys related to audio control.

Configure Bloomberg keyboard 4 or 3:

> **Caution**
>
> Editing the registry incorrectly can cause serious problems that might require you to reinstall your operating system. Citrix cannot guarantee that problems resulting from the incorrect use

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

1. Locate the following 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.

Bloomberg keyboard 3 support is available in the online plug-in 11.2 for Windows and subsequent versions.

Bloomberg keyboard 4 support is available for Windows Receiver 4.8 and later versions.

Determining if Bloomberg keyboards support is enabled:

- To check if Bloomberg keyboard support is enabled in the online plug-in, check how the Desktop Viewer reports the Bloomberg keyboard devices. If the Desktop Viewer isn't used, you can check the registry on the machine where the online plug-in is running.
- If support for Bloomberg keyboards is not enabled, the Desktop Viewer shows:
  - two devices for the Bloomberg keyboard 3, that appears as **Bloomberg Fingerprint Scanner** and **Bloomberg Keyboard Audio**.
  - one policy redirected device for Bloomberg keyboard 4. This device appears as **Bloomberg LP Keyboard 2013**.
- If support for Bloomberg keyboards is enabled, there are two devices shown in the Desktop Viewer. One appears as **Bloomberg Fingerprint Scanner** as before, and the other as **Bloomberg Keyboard Features**.
- If the driver for the Bloomberg Fingerprint Scanner device is not installed, the Bloomberg Fingerprint Scanner entry might not appear in the Desktop Viewer. If the entry is missing, the Bloomberg Fingerprint Scanner might not be available for redirection. You can still check the name of the other Bloomberg device where Bloomberg keyboards support is enabled.
- You can also check the value in the registry to know if the support is enabled: `HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\ICAClient\GenericUSB\EnableBloombergHID`

If the value doesn't exist or is 0 (zero), support for Bloomberg keyboards is not enabled. If the value is 1, support is enabled.

Enabling Bloomberg keyboard support:

> **Note:**
>
> Citrix Receiver for Windows 4.8 introduced the support for composite devices through the **SplitDevices** policy. However, you must use the Bloomberg keyboard feature instead of this policy for the Bloomberg keyboard 4.

> The support for the Bloomberg keyboard changes the way certain USB devices are redirected to a session. This support is not enabled by default.

- To enable the support during the installation time, specify the value of the **ENABLE_HID_REDIRECTION** property as TRUE at the installation command-line. For example:

  `CitrixOnlinePluginFull.exe /silent` `ADDLOCAL="ICA_CLIENT,PN_AGENT,SSON,USB"` `ENABLE_SSON="no" INSTALLDIR="c:\test"` `ENABLE_DYNAMIC_CLIENT_NAME="Yes"` `DEFAULT_NDSCONTEXT="Context1,Context2"` `SERVER_LOCATION="http://testserver.net" ENABLE_HID_REDIRECTION="TRUE"`

- To enable support after installing the online plug-in, edit the Windows Registry on the system where the online plug-in is running:

  a. Open Registry Editor.

  b. Navigate to the following key: `HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\ICA Client\GenericUSB`

  c. If the value **EnableBloombergHID** exists, modify it so that the value data is 1.

  d. If the value **EnableBloombergHID** does not exist, create a DWORD value with the name EnableBloombergHID and provide the value data as 1.

Disabling support for the Bloomberg keyboard:

You can disable support for the Bloomberg keyboard in the online plug-in as follows:

1. Open Registry Editor on the system running the online plug-in software.

2. Navigate to the following key: `HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\ICA Client\GenericUSB`
3. If the value **EnableBloombergHID** exists, modify it so that the value data is 0 (zero).

   If the value **EnableBloombergHID** doesn't exist, it indicates that the support for the Bloomberg keyboard is not enabled. In such case, you don't have to modify any registry values.

Using Bloomberg keyboards without enabling support:

- You can use the keyboard without enabling the Bloomberg keyboard support in the online plug-in. However, you cannot have the benefit of sharing the specialized functionality among multiple sessions and you might experience increased network bandwidth from audio.
- Bloomberg keyboard ordinary keys are available in the same way as any other keyboard. You don't have to take any special action.
- To use the specialized Bloomberg keys, you must redirect the Bloomberg keyboard audio device into the session. If you are using the Desktop Viewer, the manufacturer name and device name of the USB devices appears and **Bloomberg Keyboard Audio** appears for the Bloomberg Keyboard audio device.
- To use the fingerprint reader, you must redirect the device to Bloomberg Fingerprint Scanner. If the drivers for the fingerprint reader are not installed locally, the device only shows:
  - if the online plug-in is set to connect devices automatically or
  - to let the user choose whether to connect devices.

  Also, if the Bloomberg keyboard is connected before establishing the session and drivers for the fingerprint reader doesn't exist locally, then the fingerprint reader doesn't appear and isn't usable within the session.

> **Note:**
>
> For Bloomberg 3, a single session or the local system can use the fingerprint reader, and cannot be shared. Bloomberg 4 is prohibited for redirection.

> **Using Bloomberg keyboards after enabling support:**

- If you enable support for Bloomberg keyboards in the online plug-in, you have the benefit of sharing the specialized keyboard functionality with multiple sessions. You also experience less network bandwidth from the audio.

- Enabling support for the Bloomberg keyboard prevents the redirection of the Bloomberg Keyboard audio device. Instead, a new device is made available. If you are using the Desktop Viewer, this device is called Bloomberg Keyboard Features. Redirecting this device provides the specialized Bloomberg keys to the session.

Enabling the Bloomberg keyboard support only affects the specialized Bloomberg keys and the audio device. Because the ordinary keys and fingerprint reader are used in the same way as when the support is not enabled.

HDX Plug and Play USB device redirection

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

> **Important:**

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

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

To map a client COM port to a server COM port

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

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

> **Important:**

> COM port mapping isn't TAPI-compatible.

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

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

   where:

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

4. To confirm the operation, type:

   ```
   net use
   ```

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

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

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. For upgrade, the existing settings are retained while importing the latest files.
> - This feature is available only on Citrix Virtual Apps server.

> **To configure USB audio devices:**

1. Open the Citrix Workspace app Group Policy Object administrative template by running gpedit.msc.
2. Under the **Computer Configuration** node, go to **Administrative Templates \> Classic Administrative Templates (ADM) \> Citrix Components \> Citrix Workspace \> User experience**, and select **Audio through Generic USB Redirection**.
3. Edit the settings.
4. Click **Apply** and **OK**.
5. Open the cmd prompt in administrator mode.
6. Run the following command `gpupdate /force`.

Mass storage devices

For mass storage devices only, in addition to USB support, remote access is available through client drive mapping. You can configure this through the Citrix Workspace app for Windows policy **Remoting client devices** \> **Client drive mapping**. When you apply this policy, the drives on the user device automatically map to drive letters on the virtual desktop when users log on. The drives are displayed as shared folders with mapped drive letters.

The main differences between the two types of remoting policy are:

FEATURE	CLIENT DRIVE MAPPING	USB SUPPORT
Enabled by default	Yes	No
Read-only access configurable	Yes	No
Safe to remove device during a session	No	Yes, if the user clicks Safely Remove Hardware in the notification area

If you enable both Generic USB and the client drive-mapping policies and insert a mass storage device before a session starts, it is redirected using client drive mapping first, before being considered for redirection through USB support. If it is inserted after a session has started, it will be considered for redirection using USB support before client drive mapping.

Remember USB connections

Starting with Citrix Workspace app for Windows version 2409, this feature enhances the user experience when remoting USB devices to a Citrix Virtual Apps and Desktops session. While auto-redirection supports using device rules exists, this feature simplifies the process by remembering manually requested connections and reconnecting them with minimal configuration.

> **Note:**
>
> Devices that have been marked ALLOW by the administrator in the 'Client USB Device Redirection Rules (Version 2)' policy of Citrix Studio or through GPO are available for manual-remembered connection to the session. In the absence of the Version 2 policy being enabled, the devices can be marked as ALLOW in the version 1 policy rules as well. Devices marked as CONNECT are always connected, while devices marked as DENY are prohibited from connection.

Key benefits

- **Improved auto-redirection**: By remembering manual connections and associating them with the desktop resource ID, devices are redirected only in the sessions where they were initially connected.
- **Session-specific associations**: Different devices can be remembered and associated with specific sessions, providing more convenience.
- **User control**: Users can choose to automatically connect remembered devices either at session start or upon device insertion during an active session by selecting the following checkboxes in the Preferences window or by setting the appropriate GPO policy or studio policy:
  - When a session starts, connect devices automatically
  - When a new device is inserted while a session is running, connect the device automatically

These settings can also be managed using GPO policy or centrally administered through DDC policy.

To enable this feature, follow these steps:

1. Open the Registry Editor.
2. Navigate to: `Computer\HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\ICA Client\GenericUSB`.

3. Create a Registry value with the following attributes:
    - **Registry Key Name**: RememberConnections
    - **Type**: DWORD
    - **Value**: 0 (disabled) or 1 (enabled)
4. Restart the Citrix Workspace app for the changes to take effect.

> **Note:**
>
> Citrix Workspace app's default device rules include the CONNECT keyword for child devices of Bloomberg 5 keyboards. These rules are also present in the 'Client USB Device Redirection Rules (Version 2)' policy of Citrix Studio. To remember connections for the Bloomberg 5 keyboard, these rules must be modified by replacing the CONNECT keyword with ALLOW.

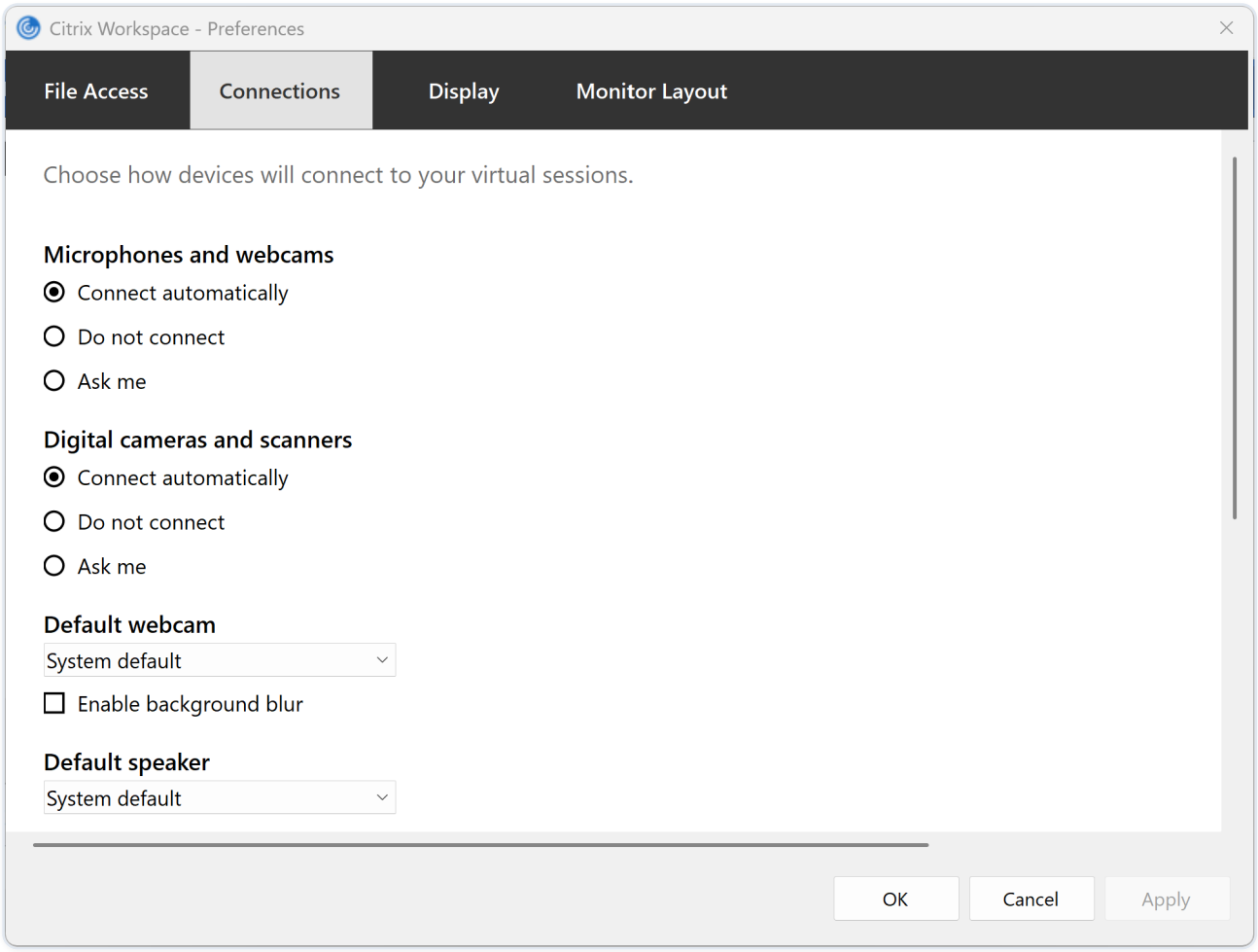
> By enabling this feature, users can enjoy a more seamless and efficient experience with USB device redirection in Citrix Virtual Apps and Desktops sessions.

Webcams

Background blurring for webcam redirection

Starting from the version 2210, Citrix Workspace app for Windows supports background blurring for webcam redirection.

Starting with version 2507.1, the background blur setting persists between sessions and reconnects. Citrix Workspace™ app remembers your preference automatically. You can enable the background blur feature by navigating to **Preferences** > **Connections** and select **Enable background blur**.



Your background blur setting remains active across all future sessions until you change it.

Support for MJPEG webcams

Starting with the 2405 version, MJPEG webcams are supported in the H264 stream. The webcam performs MJPEG compression internally which provides better image quality and a higher frame rate.

This feature is enabled by default. However, if certain Webcam doesn't support MJPEG, this feature is disabled.

Client drive-mapping

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

By default, this feature is enabled.

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

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

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

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

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

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

Disable user device mappings

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

Redirect client folders

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

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

Map client drives to host-side drive letters

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

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

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

CLIENT DRIVE LETTER	ACCESSIBLE BY THE SERVER AS
A	A
B	B
C	V
D	U

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

CLIENT DRIVE LETTER	ACCESSIBLE BY THE SERVER AS
A	A
B	B
C	C
D	D

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

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

Microphone

Citrix Workspace app supports multiple client-side microphone inputs. You can use locally installed microphones for:

- Real-time activities, such as softphone calls and Web conferences.
- Hosted recording applications, such as dictation programs.
- Video and audio recordings.

Citrix Workspace app users can select whether to use microphones attached to their device using Connection Center. Citrix Virtual Apps and Desktops and Citrix DaaS users can also use the Citrix Virtual Apps and Desktops and Citrix DaaS viewer Preferences to disable their microphones and webcams.

Group Policy

Group Policy Object administrative template

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

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

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

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

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

You can download the Citrix ADMX/ADML templates for Group Policy Editor from the Download page of Citrix.

> **Note:**

> The .admx and .adml files are for use with Windows version mentioned in the Compatibility matrix.

If Citrix Workspace app is installed with VDA, the ADMX/ADML files are typically found in the `\<installation directory>\Online Plugin\Configuration` directory.

If Citrix Workspace app is installed without the VDA, the ADMX/ADML files can be typically found in the following directory.

- For 64-bit: `C:\Program Files (x86)\Citrix\ICA Client\Configuration directory`
- For 32-bit: `C:\Program Files\Citrix\ICA Client\\Configuration directory`

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

Note:

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

FILE TYPE	FILE LOCATION
receiver.adm	<Installation Directory>\ICA Client\Configuration
receiver.admx	<Installation Directory>\ICA Client\Configuration
receiver.adml	<Installation Directory>\ICA Client\Configuration\[MUIculture]
CitrixBase.admx	<Installation Directory>\ICA Client\Configuration
CitrixBase.adml	<Installation Directory>\ICA Client\Configuration\[MUIculture]

Note:

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

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

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

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

FILE TYPE	COPY FROM	COPY TO
receiver.admx	`Installation Directory\ICA Client\Configuration\receiver.admx`	`%systemroot%\policyDefinitions`
CitrixBase.admx	`Installation Directory\ICA Client\Configuration\CitrixBase.admx`	`%systemroot%\policyDefinitions`
receiver.adml	`Installation Directory\ICA Client\Configuration\[MUIculture]receiver.adml`	`%systemroot%\policyDefinitions\[MUIculture]`
CitrixBase.adml	`Installation Directory\ICA Client\Configuration\[MUIculture]\CitrixBase.adml`	`%systemroot%\policyDefinitions\[MUIculture]`

Note:

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

Session experience

Application launch time

Use the session prelaunch feature to reduce application launch time during normal or high traffic periods, thus providing users with a better experience. The prelaunch feature allows you to create a prelaunch session. Prelaunch session is created when a user logs on to Citrix Workspace app, or at a scheduled time if the user has signed in.

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

For more information, see session prelaunch and session linger guidance in the Citrix Virtual Apps and Desktops article titled Manage delivery groups.

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

> **Note:**
>
> If the client machine has been configured to support Domain Passthrough (SSON) authentication, prelaunch is automatically enabled. If you want to use Domain Pass-through (SSON) without prelaunch, set the **EnablePreLaunch** registry key value to false.
>
> The registry locations are:

- `HKEY_LOCAL_MACHINE\Software\[Wow6432Node\]Citrix\\Dazzle`
- `HKEY_CURRENT_USER\Software\Citrix\Dazzle`

There are two types of prelaunch:

- **Just-in-time prelaunch**- prelaunch starts immediately after the user's credentials are authenticated whether it is a high-traffic period. Typically used for normal traffic periods. A user can trigger just-in-time prelaunch by restarting the Citrix Workspace app.
- **Scheduled prelaunch**- prelaunch starts at a scheduled time. Scheduled prelaunch starts only when the user device is already running and authenticated. If those two conditions are not met when the scheduled prelaunch time arrives, a session does not launch. To share network and server load, the session launches within a window when it is scheduled. For example, if the scheduled prelaunch is scheduled for 13:45, the session actually launches between 13:15 and 13:45. Typically used for high-traffic periods.

Configuring prelaunch on a Citrix Virtual Apps™ server consists of:

- creating, modifying, or deleting prelaunch applications, and
- updating user policy settings that control the prelaunch application.

You cannot customize the prelaunch feature using the `receiver.admx` file. However, you can change the prelaunch configuration by modifying registry values. Registry values can be modified during or after Citrix Workspace app for Windows installation.

- The HKEY_LOCAL_MACHINE values are written during client installation.
- The HKEY_CURRENT_USER values enable you to provide different users on the same machine with different settings. Users can change the HKEY_CURRENT_USER values without administrative permission. You can provide your users with scripts to change the values.

HKEY_LOCAL_MACHINE registry values:

For 64-bit Windows operating systems:
`HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Citrix\ICA Client\Prelaunch`

For 32-bit Windows operating systems: `HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\ICA Client\Prelaunch`

Name: **UserOverride** Type: REG_SZ

Values:

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

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

Name: **State** Type: REG_SZ

Values:

0 - Disable prelaunch.

1 - Enable just-in-time prelaunch. (Prelaunch starts after the user's credentials are authenticated.)

2 - Enable scheduled prelaunch. (Prelaunch starts at the time configured for Schedule.)

Name: **Schedule** Type: REG_SZ

Value:

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

HH:MM|M:T:W:TH:F:S:SU where HH and MM are hours and minutes. M:T:W:TH:F:S:SU is the days of the week. For example, to enable scheduled prelaunch on Monday, Wednesday, and Friday at 13:45, set Schedule as Schedule=13:45|1:0:1:0:1:0:0. The session actually launches between 13:15 and 13:45.

HKEY_CURRENT_USER registry values:

`HKEY_CURRENT_USER\SOFTWARE\Citrix\ICA Client\Prelaunch`

The **State** and **Schedule** keys have the same values as for HKEY_LOCAL_MACHINE.

Desktop Viewer

Different enterprises might have different corporate needs. Your requirements for the way users access virtual desktops might vary from user to user and as your corporate needs evolve. The user experience of connecting to virtual desktops and the extent at which the user can configure the connections depend Citrix Workspace app for Windows setup.

Use the **desktop viewer** when users need to interact with their virtual desktop. The user's virtual desktop can be a published virtual desktop, or a shared or dedicated desktop. In this access scenario, the **Desktop Viewer** toolbar functionality allows the user to open a virtual desktop in a window and pan and scale that desktop inside their local desktop. Users can set preferences and work on more than one desktop using multiple Citrix Virtual Apps and Desktops™ and Citrix DaaS connections on the same user device.

> **Note:**
>
> Use Citrix Workspace app to change the screen resolution on their virtual desktops. You can't change Screen Resolution using the Windows Control Panel.

Keyboard input in Desktop Viewer

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

Ctrl+Alt+Delete opens the security options screen, allowing you to lock the computer, sign out, switch users, or access Task Manager, just like on a local desktop.

Key presses that activate certain Microsoft accessibility features, for example, Sticky Keys, Filter Keys, and Toggle Keys are normally directed to the local computer.

You can access the Desktop Viewer toolbar's accessibility feature by pressing **Ctrl+Alt+Break**. Starting with version 2503, in the enhanced Desktop Viewer toolbar, when you press **Ctrl+Alt+Break**, the toolbar notch is highlighted. Click **Enter** to open the toolbar options, then use the **Tab** key to move forward between toolbar buttons and **Shift+Tab** key to move backward between toolbar buttons. In the old Desktop Viewer toolbar, pressing Ctrl+Alt+Break displays the Desktop Viewer toolbar buttons in a pop-up window.

Ctrl+Esc opens the **Start** menu on the remote virtual desktop when you are in Fullscreen mode, just as it does on a local Windows computer. This allows you to access the **Start** menu within your virtual session.

> **Note:**
>
> By default, if the Desktop Viewer is maximized, Alt+Tab switches focus between windows inside the session. If the Desktop Viewer is displayed in a window, Alt+Tab switches focus between windows outside the session.

> Hotkey sequences are key combinations designed by Citrix. Hotkey sequences are, for example, the Ctrl+F1 sequence reproduces Ctrl+Alt+Delete, and Shift+F2 switches applications between full-screen and windowed mode.

> **Note:**

> You can't use hotkey sequences with virtual desktops displayed in the Desktop Viewer, that is, with virtual apps and desktops sessions. However, you can use them with published applications, that is, with virtual apps sessions.

Prevent the desktop viewer window from dimming

If you have multiple Desktop Viewer windows, by default the desktops that are not active are dimmed. If users want to view multiple desktops simultaneously, information on them might be unreadable. You can disable the default behavior and prevent the **Desktop Viewer** window from dimming by editing the Registry editor.

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

- On the user device, create a REG_DWORD entry called **DisableDimming** in one of the following keys, depending on whether you want to prevent dimming for the current user of the device or the device itself. An entry exists if the Desktop Viewer has been used on the device:
  - `HKEY_CURRENT_USER\Software\Citrix\XenDesktop\DesktopViewer`
  - `HKEY_LOCAL_MACHINE\Software\Citrix\XenDesktop\DesktopViewer`

Optionally, instead of controlling dimming, you can define a local policy by creating the same REG_WORD entry in one of the following keys:

- `HKEY_CURRENT_USER\Software\Policies\Citrix\XenDesktop\DesktopViewer`
- `HKEY_LOCAL_MACHINE\Software\Policies\Citrix\XenDesktop\DesktopViewer`

Before using these keys, check whether the Citrix Virtual Apps and Desktops and Citrix DaaS™ administrator has set a policy for this feature.

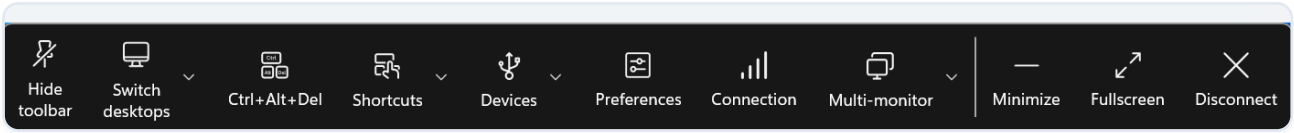
Set the entry to any non-zero value such as 1 or true.

If no entries are specified or the entry is set to 0, the **Desktop Viewer** window is dimmed. If multiple entries are specified, the following precedence is used. The first entry in this list and its value determine whether the window is dimmed:

1. HKEY_CURRENT_USER\\Software\\Policies\\Citrix\\...
2. HKEY_LOCAL_MACHINE\\Software\\Policies\\Citrix\\...
3. HKEY_CURRENT_USER\\Software\\Citrix\\...
4. HKEY_LOCAL_MACHINE\\Software\\Citrix\\...

Enhanced Desktop Viewer toolbar

Starting with the 2503 version, Citrix Workspace™ app for Windows provides an enhanced Desktop Viewer toolbar.



The enhanced Desktop Viewer toolbar provides the following options:

- **Show or hide toolbar**: Click this button to show or hide the Desktop Viewer toolbar.
- **Switch desktop**: Click this button to see the available open desktops. You can switch to another desktop by clicking the desktop that you want to access. The opened desktop shows in the front.
- **Ctrl+Alt+Del**: Click this button to bring up the task manager on your virtual desktop.
- **Shortcuts**: Click this button to see the available shortcuts. The following are the available shortcuts:
    - **Start menu**: Click to access the start menu on the virtual desktop.
    - **Switch app**: Click this button to see the available open apps. You can switch to another app by clicking the app that you want to access.
    - **Devices**: Click this button to access the devices you have connected.
    - **Preferences**: Click this button to access the options in the Preferences section and edit your preferences.
    - **Connection**: Click this button to analyze the connection strength with real-time stats of your connection.
    - **Multi-monitor**: Click this button to navigate to the different options of extending your session across multiple monitors.

- **Minimize**: Click the **Minimize** button to minimize the current virtual desktop session that you are using.

  > **Note:**
  >
  > In the old Desktop Viewer toolbar, the **Home** option minimized all virtual desktop sessions on the same monitor.

- **Fullscreen or Restore**: Click the **Fullscreen** button to expand the desktop session to full screen.Click the **Restore** button to restore to the window mode. In the old Desktop Viewer toolbar, the corresponding option for **Fullscreen or Restore** is labeled **Fullscreen or Window**.
- **Disconnect / Sign out**: Click this button to sign out or to disconnect from a virtual session.

You can drag the toolbar across the screen and snap it to any edge of the screen. It supports both vertical and horizontal layouts.

Limitation

If you are using **Windows Server OS 2019**, the new Desktop Viewer toolbar is disabled due to an issue with installing **WindowsAppSDK version 1.6.5**. For more information, see the Microsoft documentation. As a result, the legacy Desktop Viewer is enabled by default. Admins or users can enable the sideloading policy and install the **WindowsAppSDK**. After that, enable the new Desktop Viewer toolbar through the registry by setting the **REG_DWORD** entry called **WindowsAppSdkInstalled** to **1** at `HKEY_LOCAL_MACHINE\Software\Citrix\XenDesktop\DesktopViewer`.

Status indicator time-out

You can change the amount of time the status indicator displays when a user is launching a session.

To alter the time-out period, do the following steps:

1. Launch the Registry Editor.
2. Navigate to the following path:
   - On a 64-bit: `HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Citrix\ICA CLIENT\Engine`
   - On a 32-bit: `HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\ICA CLIENT\Engine\`

3. Create a registry key as follows:

    - Type: REG_DWORD
    - Name: `SI INACTIVE MS`
    - Value: 4, if you want the status indicator to disappear sooner.

When you configure this key, the status indicator might appear and disappear frequently. This behavior is as designed. To suppress the status indicator, do the following:

1. Launch the Registry Editor.
2. Navigate to the following path:

    - On a 64-bit: `HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Citrix\ICA CLIENT\`
    - On a 32-bit: `HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\ICA CLIENT\`

3. Create a registry key as follows:

    - Type: REG_DWORD
    - Name: `NotificationDelay`
    - Value: Any value in millisecond (for example, 120000)

Customization of Desktop Viewer toolbar

Starting with Citrix Workspace app for Windows 2409 version, you can customize the options on the **Desktop Viewer** toolbar using the Global App Configuration service, Group Policy Editor, or any third-party Endpoint Management software capable of pushing Windows registry keys.

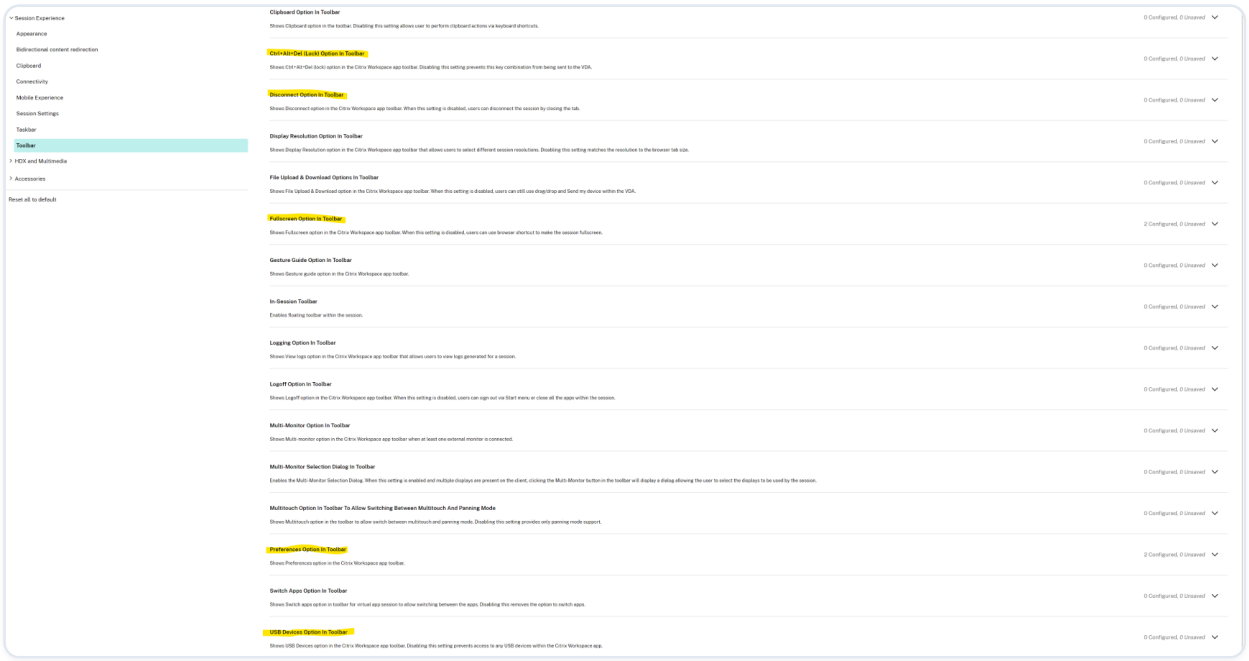
Using GACS

To configure the customization of the **Desktop Viewer** toolbar through the GACS Admin UI, do the following:

1. Sign in to citrix.cloud.com with your credentials.

> **Note:**
>
> Refer to the Sign Up for Citrix Cloud article for step-by-step instructions to create a Citrix Cloud account.

2. Upon authentication, click the menu button in the top left corner and select **StoreFront Cloud**. The StoreFront Cloud screen appears.
3. Click **App Configuration** > **Citrix Workspace app**.
4. Select the **Windows** checkbox.
5. You can now update the settings under **Session Experience** > **Toolbar**.

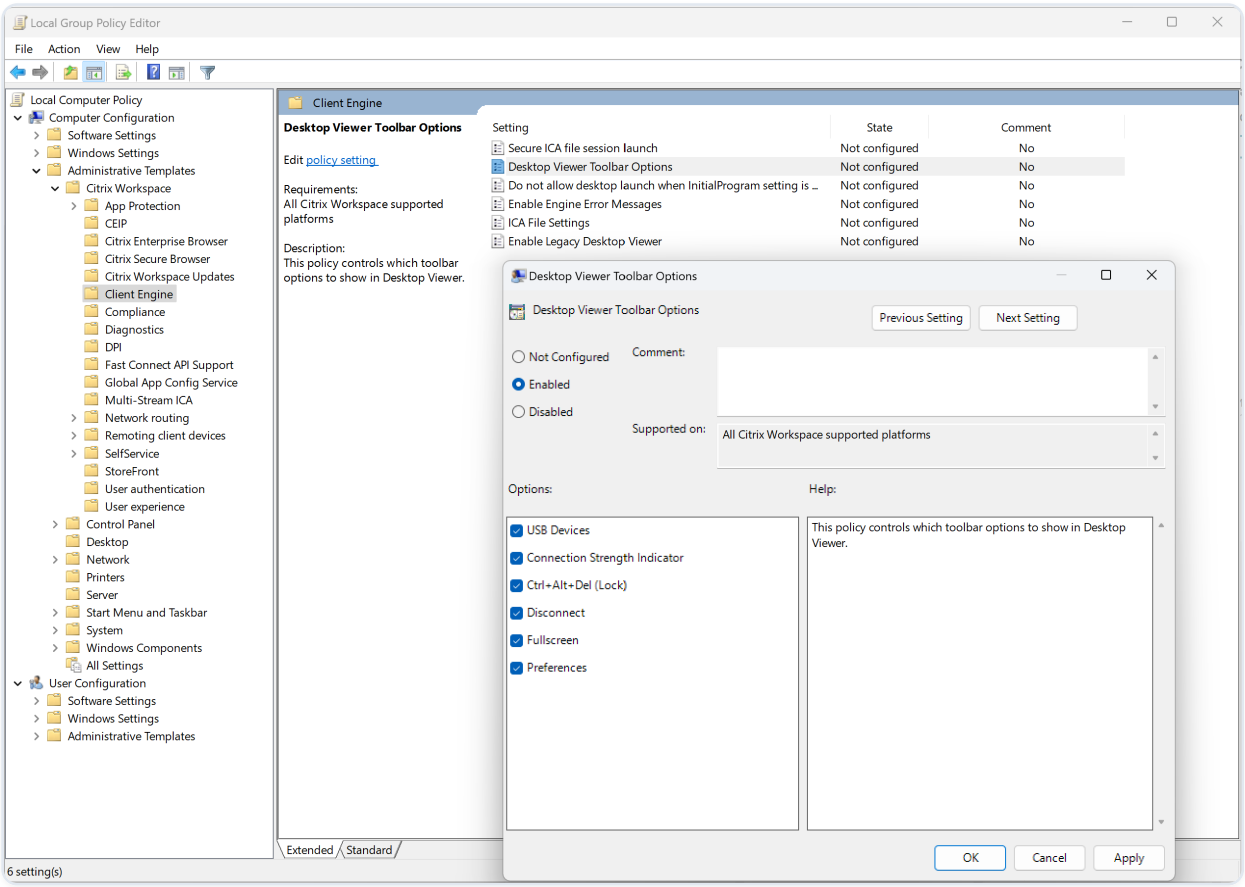


For more information, see the Global App Configuration service documentation.

Using Group Policy Editor

To customize the options on the **Desktop Viewer** toolbar, do the following:

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** > **Client Engine** and select **Desktop Viewer Toolbar Options**.



3. Select the **Enabled** checkbox.
4. Select the required checkboxes from the **Options** section.
5. Click **OK**.

Connection Strength Indicator on Desktop Viewer toolbar

Starting with version 2409, Citrix Workspace app for Windows now supports the Connection Strength Indicator (CSI) on the **Desktop Viewer** toolbar. This feature displays a network strength icon that alerts you of network issues. You can click the indicator to view real-time connection statistics for the client and VDA, and copy diagnostic information to share with IT for advanced troubleshooting.

Benefits:

- Immediate feedback: The network strength icon gently nudges users when network issues are detected.
- Enhanced troubleshooting: Real-time stats and diagnostics help users and IT teams quickly identify and resolve connectivity issues.

Prerequisites:

- This feature is only available when a session opened using:
  - VDA 2407 or later
  - VDA 2402 LTSR CU1 or later
- The Supportability Virtual Channel must be enabled.

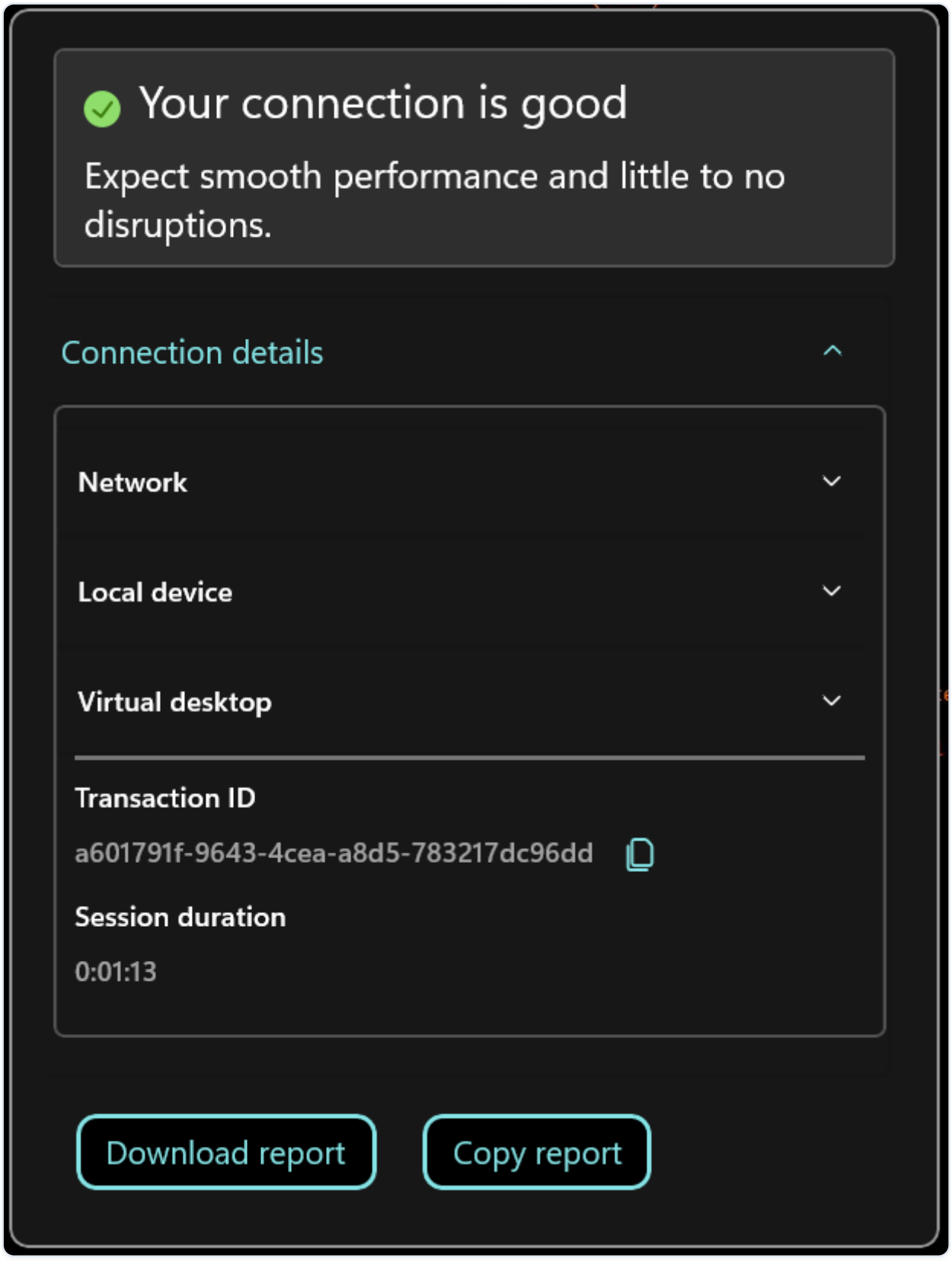
This feature is enabled by default. When you open the session, you can see the **Connection Details** icon on the **Desktop Viewer** toolbar.

The connection strength indicator on the **Desktop Viewer** toolbar provides users with immediate feedback on their network connectivity and offers detailed real-time stats for enhanced troubleshooting. This feature aims to improve user experience and reduce the time spent on resolving connectivity issues.

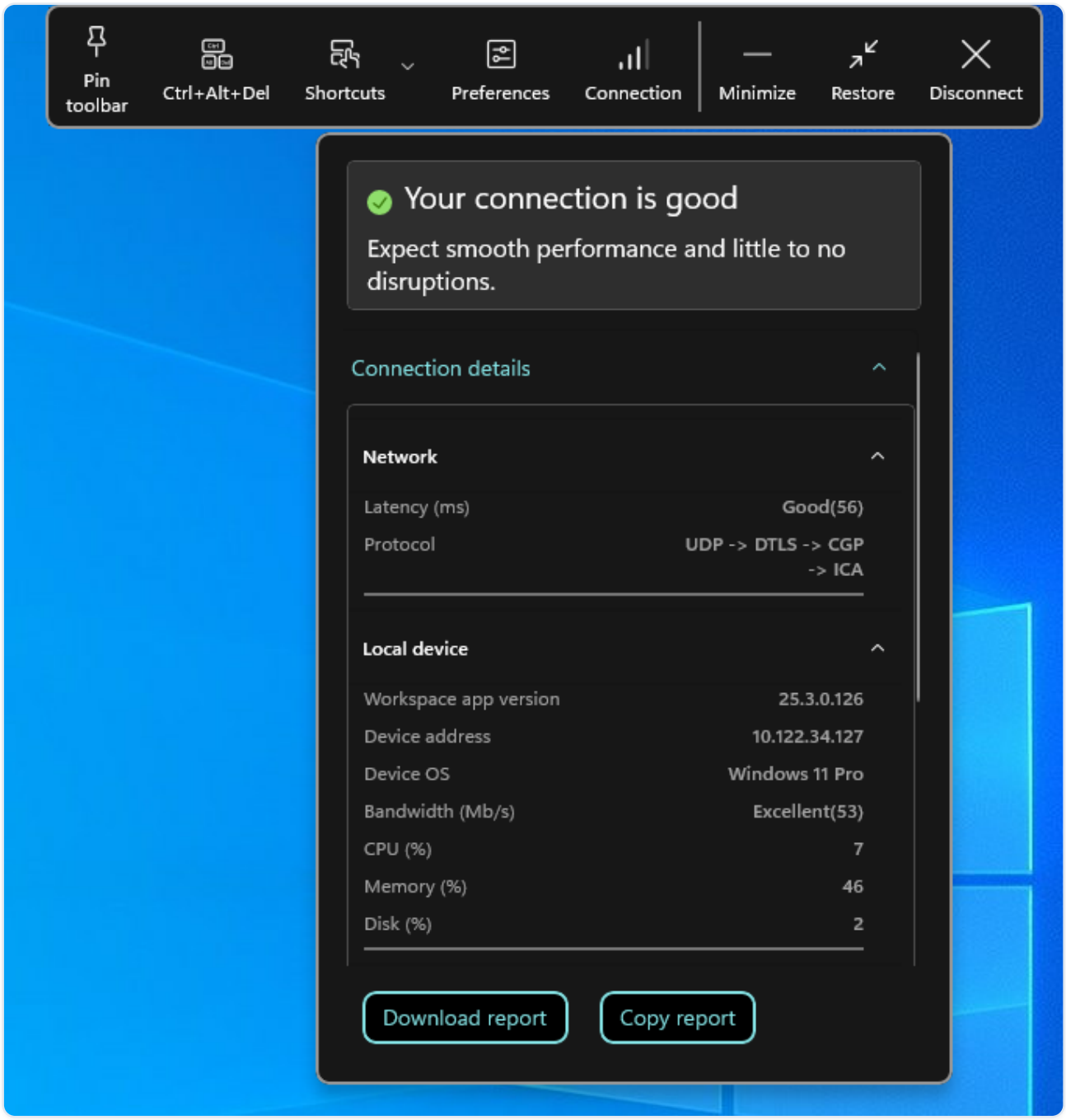
Enhancement to connection strength indicator on Desktop Viewer toolbar:

Starting with version 2503, the **Connection Strength Indicator** on the **Desktop Viewer** toolbar is enhanced with the following features:

- **Enhanced user experience**: Provides a more intuitive and user-friendly interface.
- **New stats including Wi-Fi strength**: Displays real-time Wi-Fi strength for better connectivity insights.
- **Additional details about your device**: Includes information such as CPU, memory, and disk utilization.
- **Proactive notifications with options to snooze**: Alerts users when connection strength drops, with the ability to snooze notifications.
- **Recommendations to resolve issues**: Offers actionable suggestions to improve connection strength when it drops below good.
- **Historic view of the connection strength**: The logs downloaded from the CSI provides a 5 minute history of the end user's connection strengths.



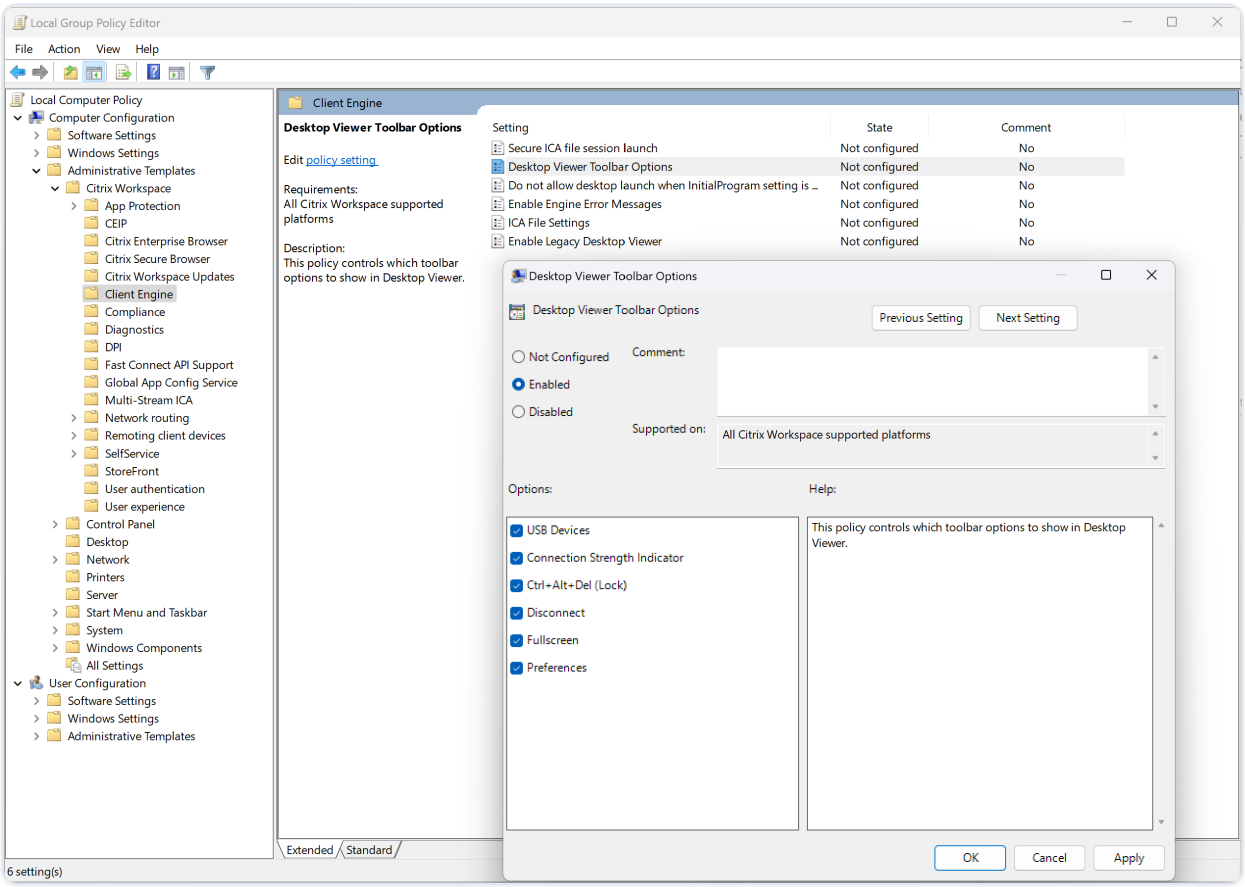
When clicked on Connection details, you can view the following image:



Disable connection strength indicator:

To disable connection strength indicator feature, do the following:

1. Open the Citrix Workspace app Group Policy Object administrative template by running `gpedit.msc`.
2. Under the **Computer Configuration** node, go to **Administrative Templates** > **Citrix Components** > **Citrix Workspace** > **Client Engine**.
3. Select the **Desktop Viewer Toolbar Options** policy.



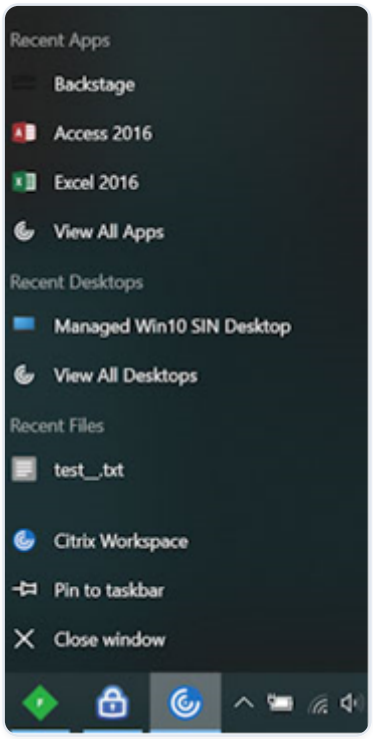
4. Select **Disabled** to disable the Desktop Viewer Toolbar options.
5. Select **Connection Strength Indicator** from the **Options** section to display the Connection Strength Indicator on the Desktop Viewer toolbar.

Enhanced virtual desktop screen resizing experience

Starting with the 2409 version, Citrix Workspace app for Windows ensures a smooth transition and prevents dark screens and flickers when resizing or stretching your virtual desktop screen. This feature is enabled by default.

Quick access to resources

Starting from the 2205 release, you can get quick access to your recently used apps and desktops. Right-click on the Citrix Workspace app icon in the taskbar to view and open the recently used resources from the pop-up menu.



Support to open Citrix Workspace app in maximized mode

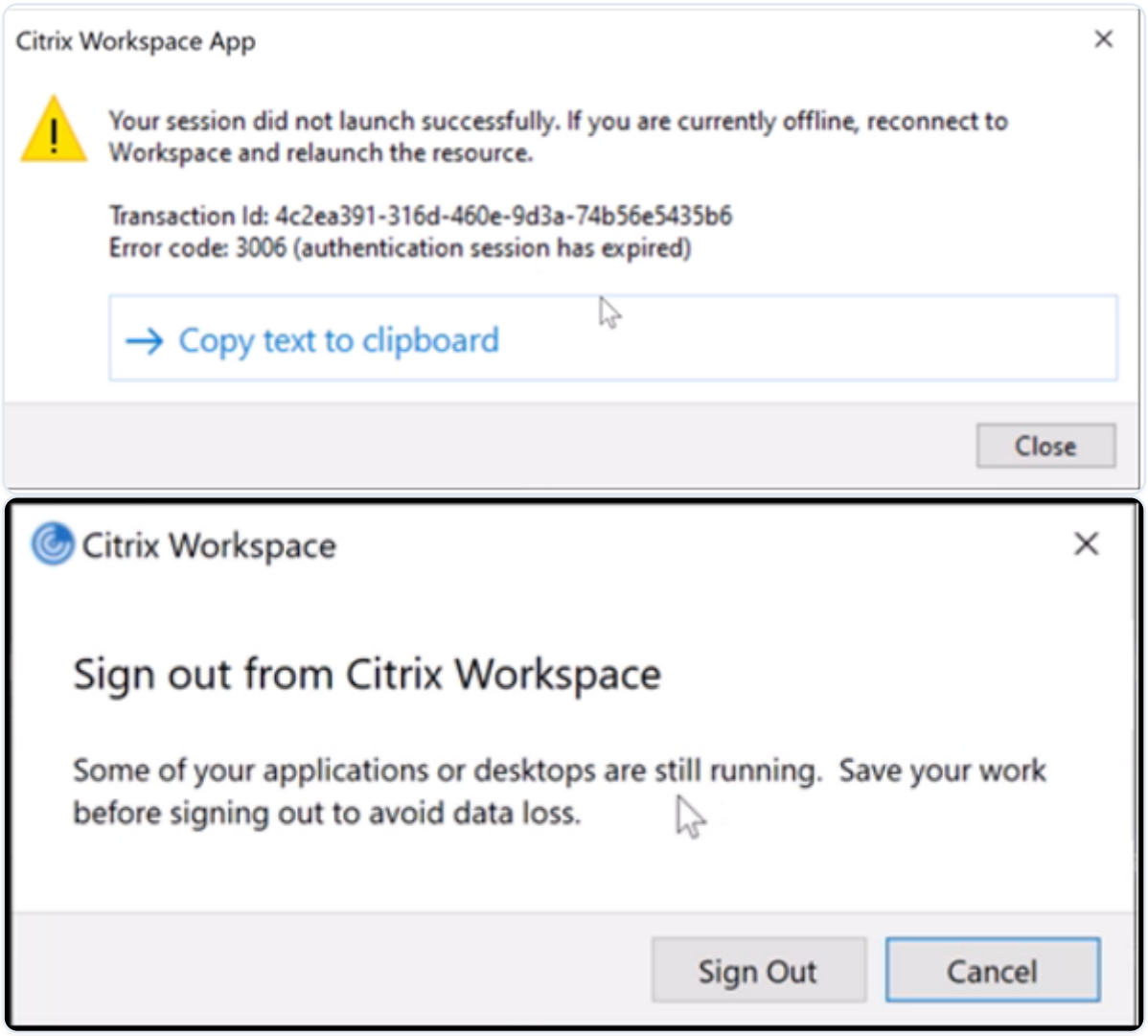
Starting from the 2205 release, you can choose to open the Citrix Workspace app in maximized mode. Instead of maximizing the Citrix Workspace app manually every time, you can set the `maximise workspace window` property in the Global App Configuration Service to enable the Citrix Workspace app to open in the maximized mode by default.

For more information about the Global App Configuration Service, see Getting Started.

Improved reconnection experience after connection lease file expiry

Previously, there was no notification to the end user when the connection lease file and authentication token expired.

Starting from the 2212 release, you are prompted with an error message and a consent dialog box. The consent dialog box appears only when you have resources running in the session. If there are no resources running, only an error dialog box appears. You are signed out without being prompted with the consent dialog box.



You can click **Sign Out** to sign out from the current Citrix Workspace app session or click **Cancel** to continue with the session.

> **Note:**
>
> Save your data before clicking **Sign Out**.

Disabling the "Exiting Full Screen Mode" tip prompt

Starting with Citrix Workspace app for Windows 2409, you can suppress the "Exiting Full Screen Mode" tip prompt that appears during HDX sessions using the Registry Editor.

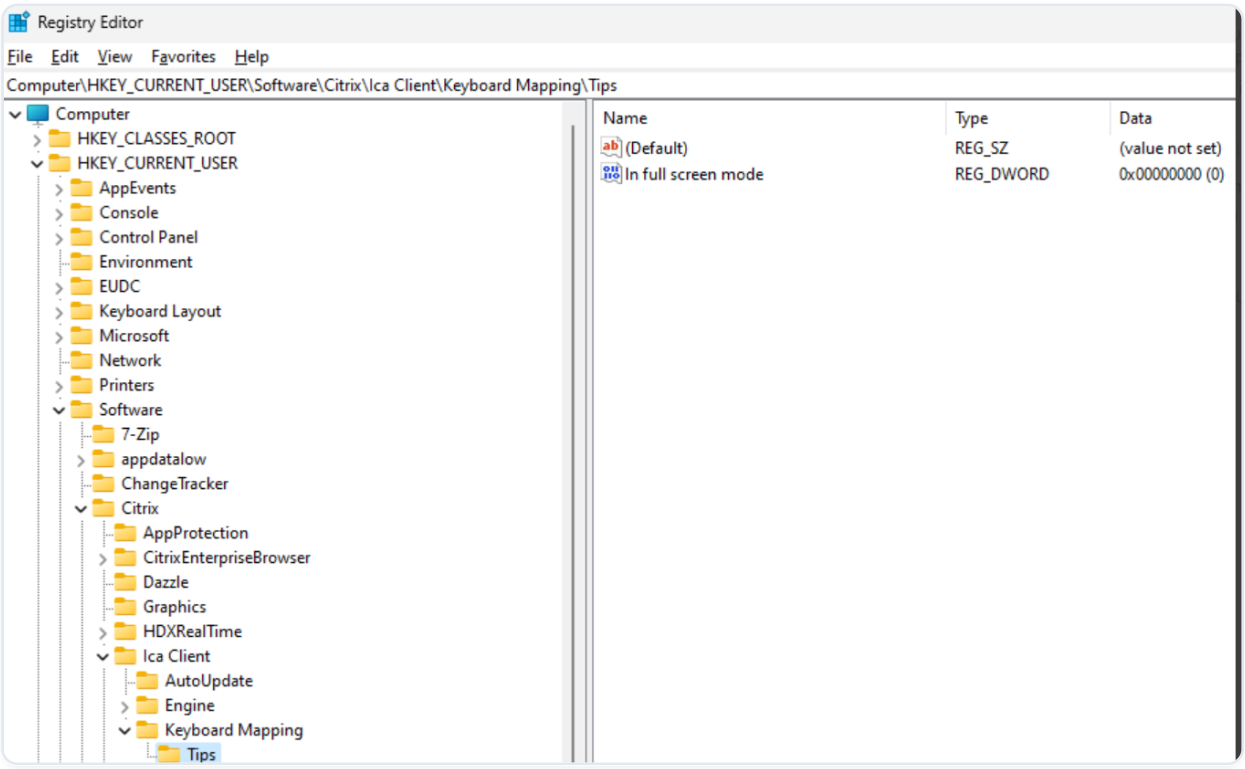
You can do it using the Registry Editor.

You can navigate to the following registry entry as an administrator and set the value as suggested:

- Path:

  - On 32-bit systems: `HKEY_LOCAL_MACHINE\Software\Citrix\Ica Client\Keyboard Mapping\Tips`
  - On 64-bit systems: `HKEY_LOCAL_MACHINE\Software\WOW6432Node\Citrix\Ica Client\Keyboard\Tips`
  - On end user systems: `HKEY_CURRENT_USER\Software\Citrix\Ica Client\Keyboard Mapping\Tips`

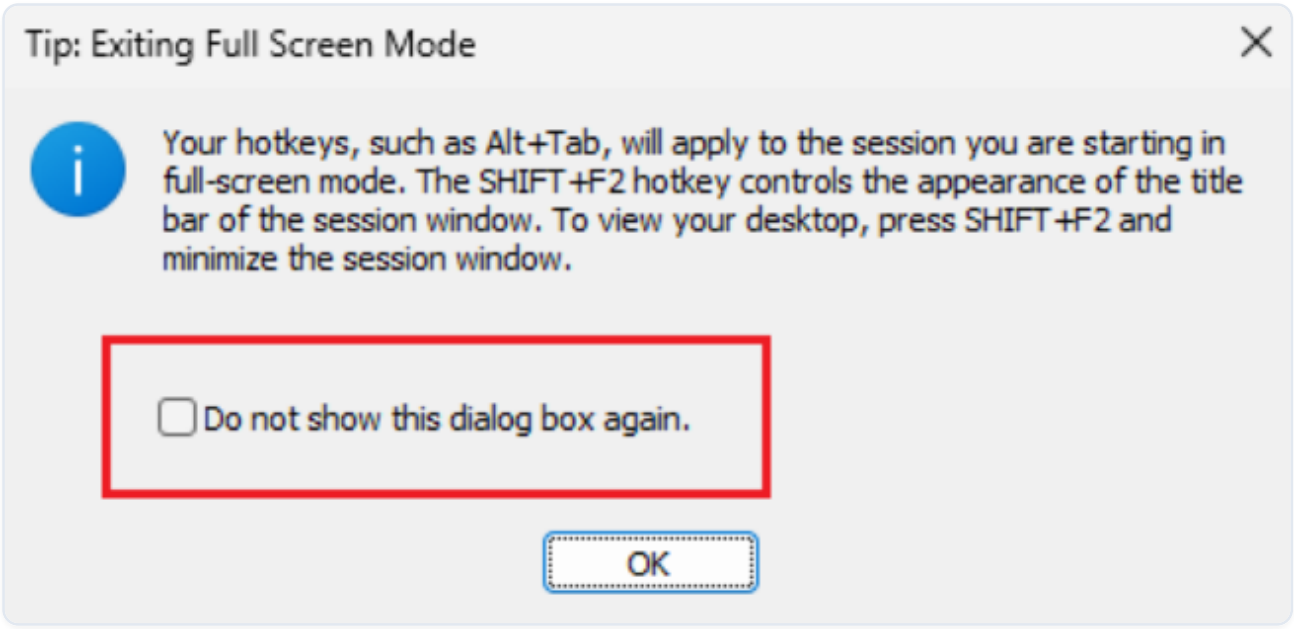
- Name: `In full screen mode`
- Type: `DWORD`
- Value: Other than 0



Note:

If the `In full screen mode` key value data is `0` or not configured, the tip is displayed.

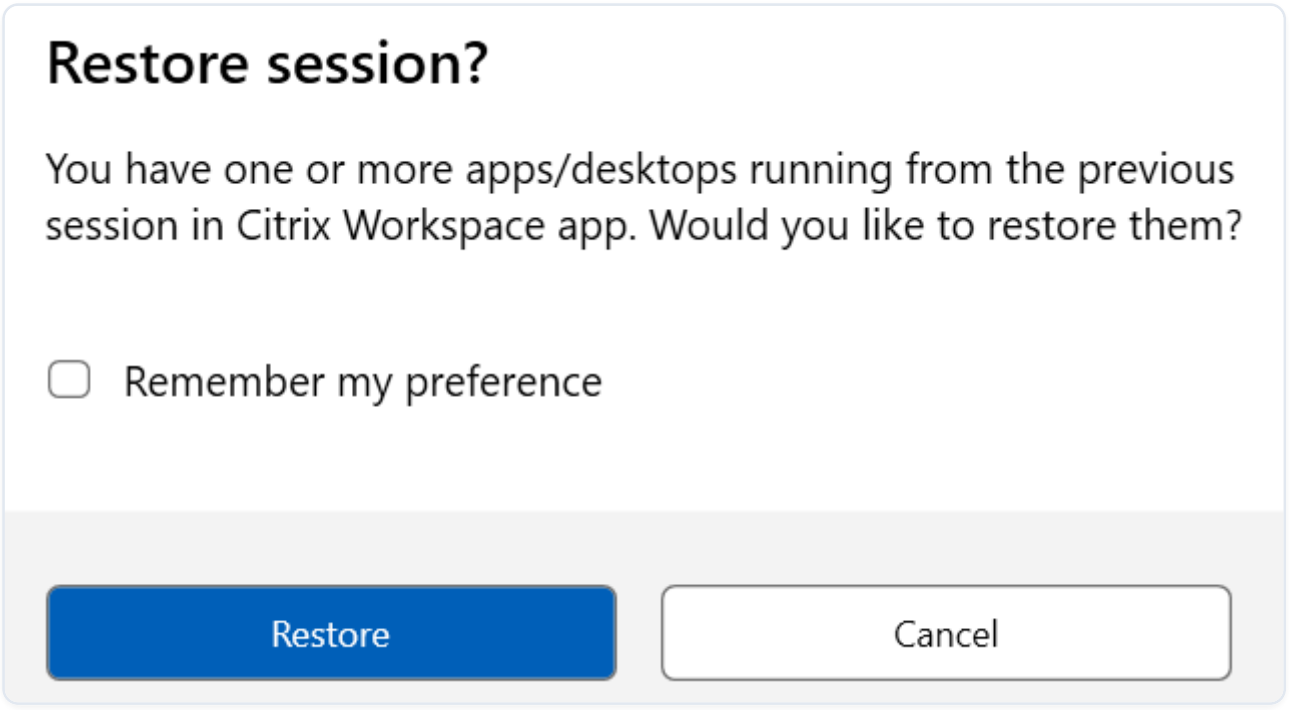
You can also select the checkbox in the following prompt, which in turn updates the `In full screen mode` value to a value other than zero.



Improved virtual apps and desktops reconnection experience

Citrix Workspace 2302 release provides an enhanced user experience while reconnecting to virtual apps and desktops from which you got disconnected.

When Citrix Workspace app attempts to refresh the disconnected Citrix Workspace app or start new virtual apps or desktops as a part of the Workspace Control feature, the following prompt appears:



Click **Restore** to reconnect to open new and disconnected virtual apps and desktops. If you want to start only newly selected apps and desktops, click **Cancel**.

You can also select **Remember my preference** to apply the selected preference for the next login. To reset your selected preferences, you must reset Citrix Workspace app.

The preceding new **Restore session?** prompt appears only if:

- the user tries to start an app belonging to a workspace store,
- admin policies or app config settings are not configured for the Workspace Control feature,
- Workspace Control Reconnect options are set to default on the client.

Note:

Reconnect settings in the **Reconnect Options** takes precedence over the preferences set in the dialog box. For more information, see Configure reconnect options using Advanced Preferences dialog.

Sustainability initiative from Citrix Workspace app

Note:

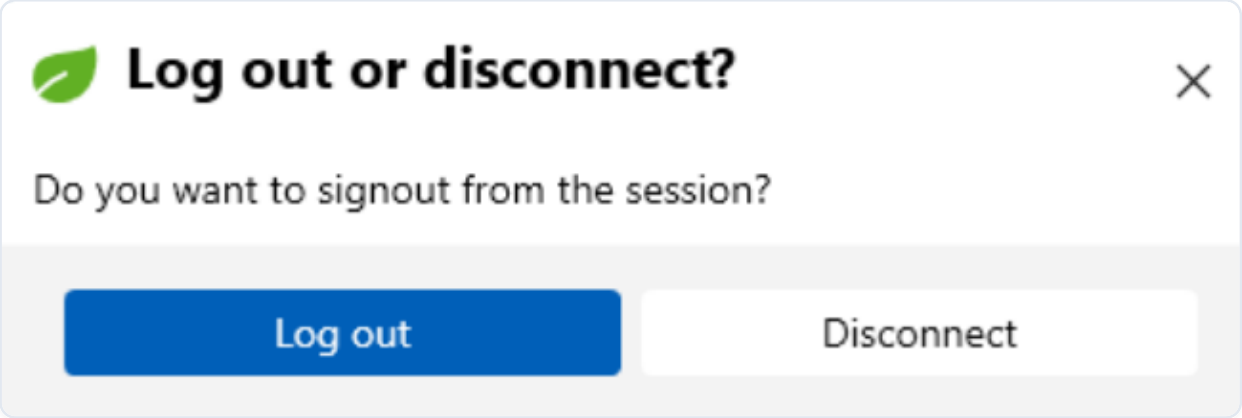
- This feature is available for native launches (cloud and on-premises) from the Citrix Workspace app 2309 version onwards.
- It is available for hybrid launches on cloud from the Citrix Workspace app 2403 version onwards.
- Starting from the Citrix Workspace app 2409 version onwards, the same keyword is used for both hybrid and native launches.
- Starting from the Citrix Workspace app 2409 version onwards, the `LogoffOnClose` and `PromptMessage` keywords are no longer supported.

When this feature is enabled, a prompt is displayed to sign out from the desktop session when a user closes a virtual desktop. This feature might help conserve energy if there are Windows OS policies that are used to shut down VMs when no users are logged in.

To enable this feature, do the following:

1. Navigate to Citrix Studio.

2. Click **Delivery Groups** from the left navigation pane.
3. Select the required VDA from the **Delivery Group** section.
4. Click the **Edit** icon. The **Edit Delivery Group** page appears.
5. Click **Desktops** from the left navigation pane.
6. Select the required VDA where you must add the keywords.
7. Click **Edit**. The **Edit Desktop** page appears.
8. Set the `ICA-LogOffOnClose` keyword to `true` in the **Description** field.
9. Click **OK**. The following dialog box appears when you close the virtual desktop.



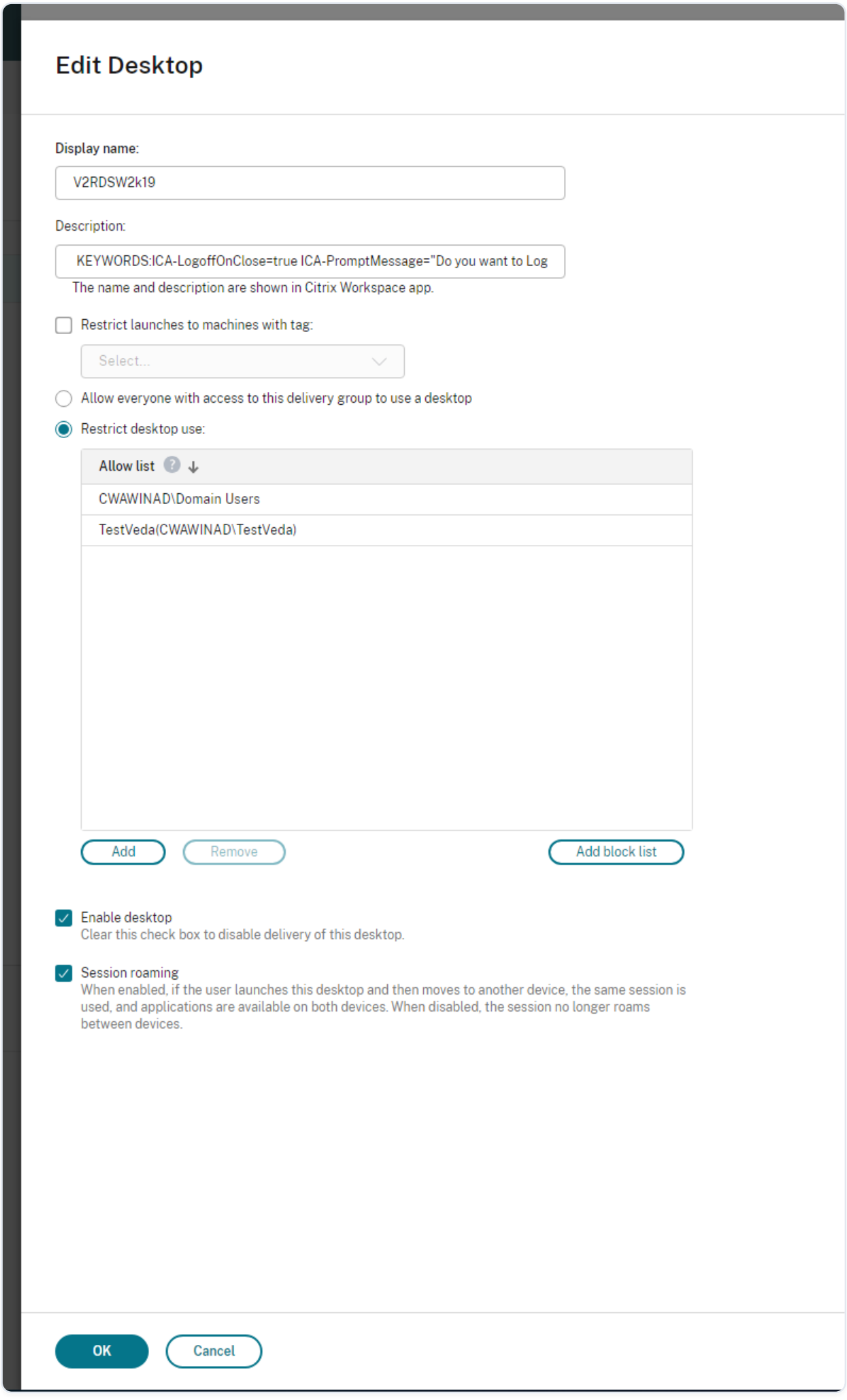
Customizing the text in the Save Energy screen

You can also customize the text in the **Save energy** screen.

1. Follow steps 1–8 in the preceding section.
2. Set the `ICA-PromptMessage` keyword to the required text in the **Description** field.
3. Set the `ICA-Title` keyword to the required text in the **Description** field.
4. Set the `ICA-Icon` keyword to `true` or `false`.

> **Note:**
>
> The maximum number of characters allowed in the `ICA-PromptMessage` keyword is 200, and in the `ICA-Title` keyword is 30.
>
> **Example:**

```
KEYWORDS:ICA-LogOffOnClose=true ICA-PromptMessage="Do you want to sign
out from the session?" ICA-Title="Sign out or disconnect" ICA-Icon=true
```


Edit Desktop
Display name:
V2RDSW2k19
Description:
KEYWORDS:ICA-LogoffOnClose=true ICA-PromptMessage="Do you want to Log
The name and description are shown in Citrix Workspace app.
Restrict launches to machines with tag:
Select...
Allow everyone with access to this delivery group to use a desktop
Restrict desktop use:
Allow list
CWAWINAD\Domain Users
TestVeda(CWAWINAD\TestVeda)
Add
Remove
Add block list
Enable desktop
Clear this check box to disable delivery of this desktop.
Session roaming
When enabled, if the user launches this desktop and then moves to another device, the same session is used, and applications are available on both devices. When disabled, the session no longer roams between devices.
OK
Cancel

The keywords are assigned by default for new desktop machines assigned to the group. For existing desktop machines, you must run the following PowerShell commands for changes to apply:

```
$dg = Get-BrokerDesktopGroup -Name '<group name>' -Property
'Name','Uid'



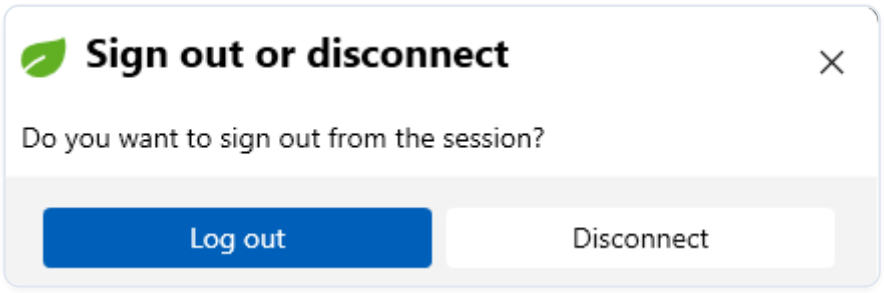
$apr = @( Get-BrokerAssignmentPolicyRule -DesktopGroupUid $dg.Uid
-Property 'Description' )



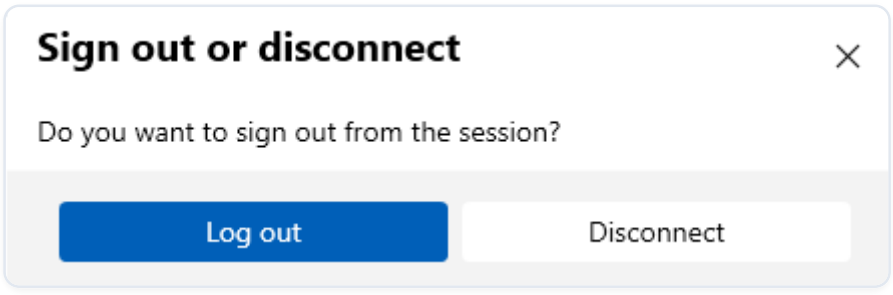
Get-BrokerMachine -DesktopGroupUid $dg.Uid -IsAssigned $true | Set-
BrokerMachine -Description $apr[0].Description
```

With this PowerShell script, it's possible to have multiple assignment policy rules for a single Delivery Group. Using Citrix Studio also, you can configure multiple Assignment policy rules, each with a unique description value, and a possible set of different keywords.

5. Click **OK**. The following dialog box appears when you close the virtual desktop.



When ICA-Icon=false



Manage workspace control reconnect

Workspace control lets applications follow users as they move between devices. For example, workspace control enables clinicians in hospitals to move from workstation to workstation without having to restart their applications on each device. For Citrix Workspace app, you manage workspace control on client devices using the Global App Config Service, Group Policy or modifying the registry.

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

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

WSCReconnectMode key settings for Citrix Workspace app:

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

Disable workspace control

To disable workspace control, create the following key:

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

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

Name: **WSCReconnectModeUser**

Type: REG_SZ

Value data: `0`

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

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

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

Name: **WSCReconnectMode**

Type: REG_SZ

Value data: `0`

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

Registry keys for 32-bit machines

Registry key: `WSCSupported`

Value: `True`

Key path:

```
-  HKEY_CURRENT_USER\Software\Citrix\Dazzle

-  HKEY_CURRENT_USER\Software\Citrix\Receiver\SR\Store" + primaryStoreID +
\Properties

-  HKEY_LOCAL_MACHINE\Software\Policies\Citrix\Dazzle

-  HKEY_LOCAL_MACHINE\Software\Citrix\Dazzle
```

Registry key: WSCReconnectAll

Value: `True`

Key path:

```
- `HKEY_CURRENT_USER\Software\Citrix\Dazzle`

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

- `HKEY_LOCAL_MACHINE\Software\Policies\Citrix\Dazzle`

- `HKEY_LOCAL_MACHINe\Software\Citrix\Dazzle`
```

Registry key: WSCReconnectMode

Value: `3`

Key path:

```
-  HKEY_CURRENT_USER\Software\Citrix\Dazzle

-  HKEY_CURRENT_USER\Software\Citrix\Receiver\SR\Store" + primaryStoreID +
\Properties

-  HKEY_LOCAL_MACHINE\Software\Policies\Citrix\Dazzle

-  HKEY_LOCAL_MACHINE\Software\Citrix\Dazzle
```

Registry key: WSCReconnectModeUser

Value: The registry isn't created during installation.

Key path:

```
- HKEY_CURRENT_USER\Software\Citrix\Dazzle

- HKEY_CURRENT_USER\Software\Citrix\Receiver\SR\Store" + primaryStoreID+
\Properties

- HKEY_LOCAL_MACHINE\Software\Policies\Citrix\Dazzle

- HKEY_LOCAL_MACHINE\Software\Citrix\Dazzle
```

Registry keys for 64-bit machines

Registry key: `WSCSupported`

Value: `True`

Key path:

```
- HKEY_CURRENT_USER\Software\Citrix\Dazzle

- HKEY_CURRENT_USER\Software\Citrix\Receiver\SR\Store" + primaryStoreID +
\Properties

- HKEY_LOCAL_MACHINE\Software\Wow6432Node\Policies\Citrix\Dazzle

- HKEY_LOCAL_MACHINE\Software\Wow6432Node\Citrix\Dazzle
```

Registry key: `WSCReconnectAll`

Value: `True`

Key path:

```
-  HKEY_CURRENT_USER\Software\Citrix\Dazzle

-  HKEY_CURRENT_USER\Software\Citrix\Receiver\SR\Store" + primaryStoreID +
\Properties

-  HKEY_LOCAL_MACHINE\Software\Wow6432Node\Policies\Citrix\Dazzle

-  HKEY_LOCAL_MACHINE\Software\Wow6432Node\Citrix\Dazzle
```

Registry key: WSCReconnectMode

Value: `3`

Key path:

```
-  HKEY_CURRENT_USER\Software\Citrix\Dazzle

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

```
- HKEY_LOCAL_MACHINE\Software\Wow6432Node\Policies\Citrix\Dazzle

- HKEY_LOCAL_MACHINE\Software\Wow6432Node\Citrix\Dazzle
```

Registry key: WSCReconnectModeUser

Value: The registry isn't created during installation.

Key path:

```
- HKEY_CURRENT_USER\Software\Citrix\Dazzle

- HKEY_CURRENT_USER\Software\Citrix\Receiver\SR\Store" + primaryStoreID+
\Properties

- HKEY_LOCAL_MACHINE\Software\Wow6432Node\Policies\Citrix\Dazzle

- HKEY_LOCAL_MACHINE\Software\Wow6432Node\Citrix\Dazzle
```

Automated sign-out on session disconnect

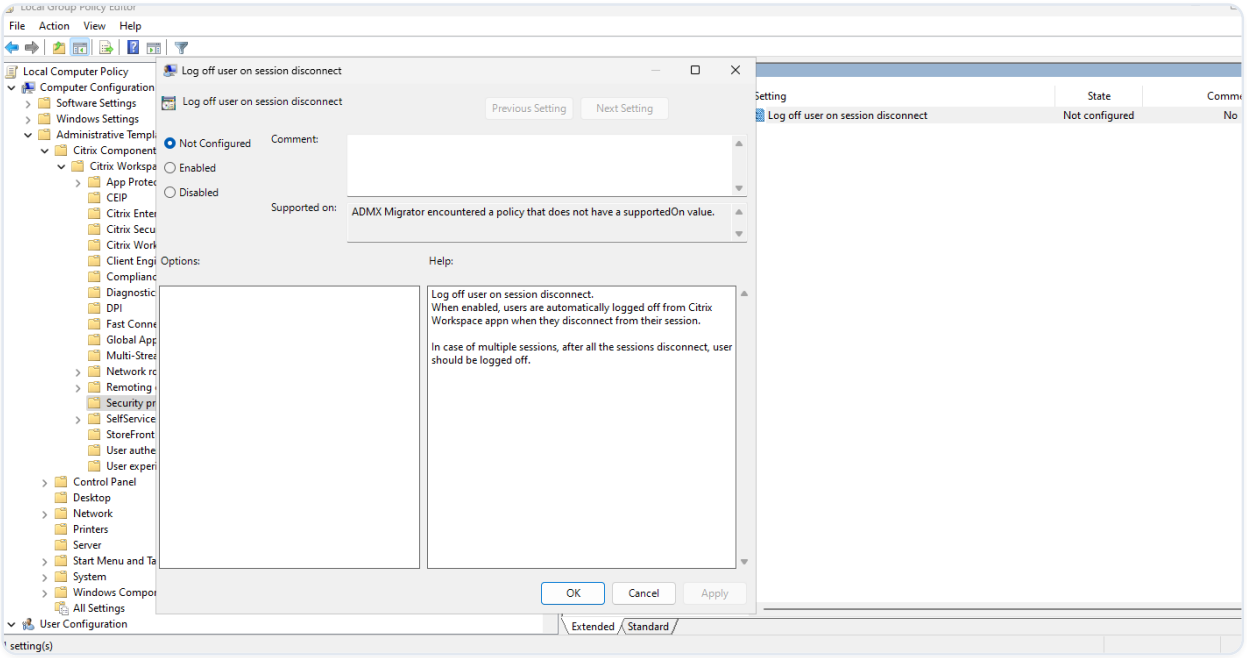
Beginning with 2507.1 release, Citrix Workspace app can automatically sign out users when their session is disconnected. This feature is designed for kiosk environments to enhance security on shared devices.

You can enable this feature through Group Policy Object (GPO) or Global App Configuration service (GACS).

Using Group Policy Editor:

To enable the automatic sign out of users when their session is disconnected through GPO, do the following:

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 > Security preferences and select **Log off user on session disconnect**.



3. Select the **Enabled** checkbox.
4. Click **OK**.

Using GACS:

To enable the automatic sign out of users when their session is disconnected through GACS, do the following:

1. Sign in to citrix.cloud.com with your credentials.

> **Note:**
>
> Refer to the Sign Up for Citrix Cloud article for step-by-step instructions to create a Citrix Cloud account.

2. Upon authentication, click the menu button in the top left corner and select **StoreFront Cloud**. The StoreFront Cloud screen appears.
3. Click **App Configuration** > **Citrix Workspace app**.
4. Select the **Windows** checkbox.
5. You can now update the settings under **Security preferences** > **Log off user on session disconnect**.

For more information, see the Global App Configuration service documentation.

Persistent session in Citrix Workspace app

Starting with the 2503 version, if you enable the Persistent session feature, Citrix Workspace app automatically detects session termination and relaunches the application or desktop without any user intervention when the application or desktop session logs out or disconnects.

This feature ensures uninterrupted application or desktop availability, improving user experience and productivity.

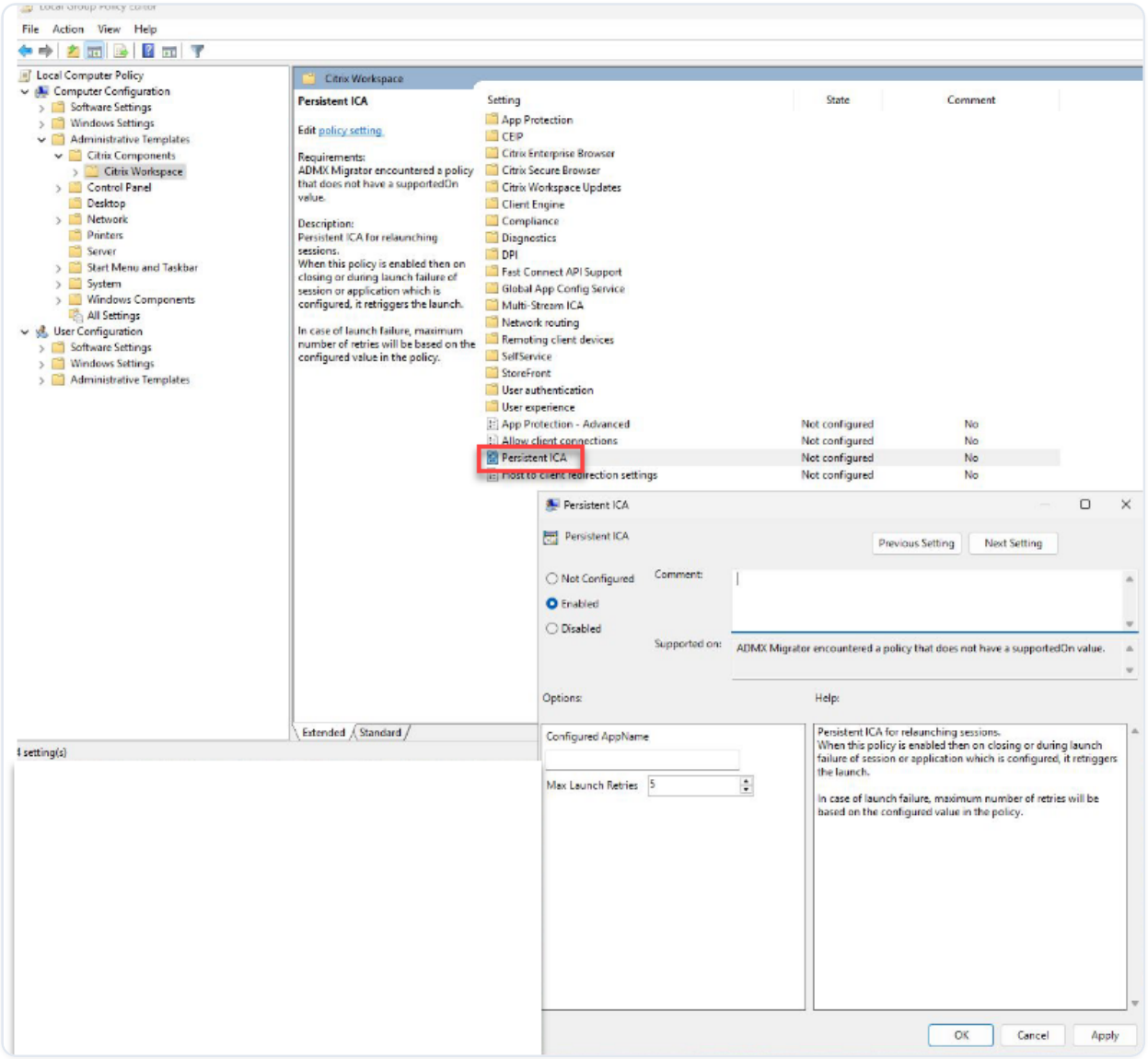
> **Note:**
>
> - This feature is supported only on the native Citrix Workspace app.
> - Persistent ICA Session is not supported for Workstation VDA incase of session roaming.

> Administrators can enable this feature through a Group Policy Object (GPO) policy. The policy allows admins to configure a specific application or desktop as a persistent resource and define the number of retries if there is a resource launch failure:

- **Default retries**: 5
- **Retry range**: 0–10

Enabling persistent session feature using GPO:

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

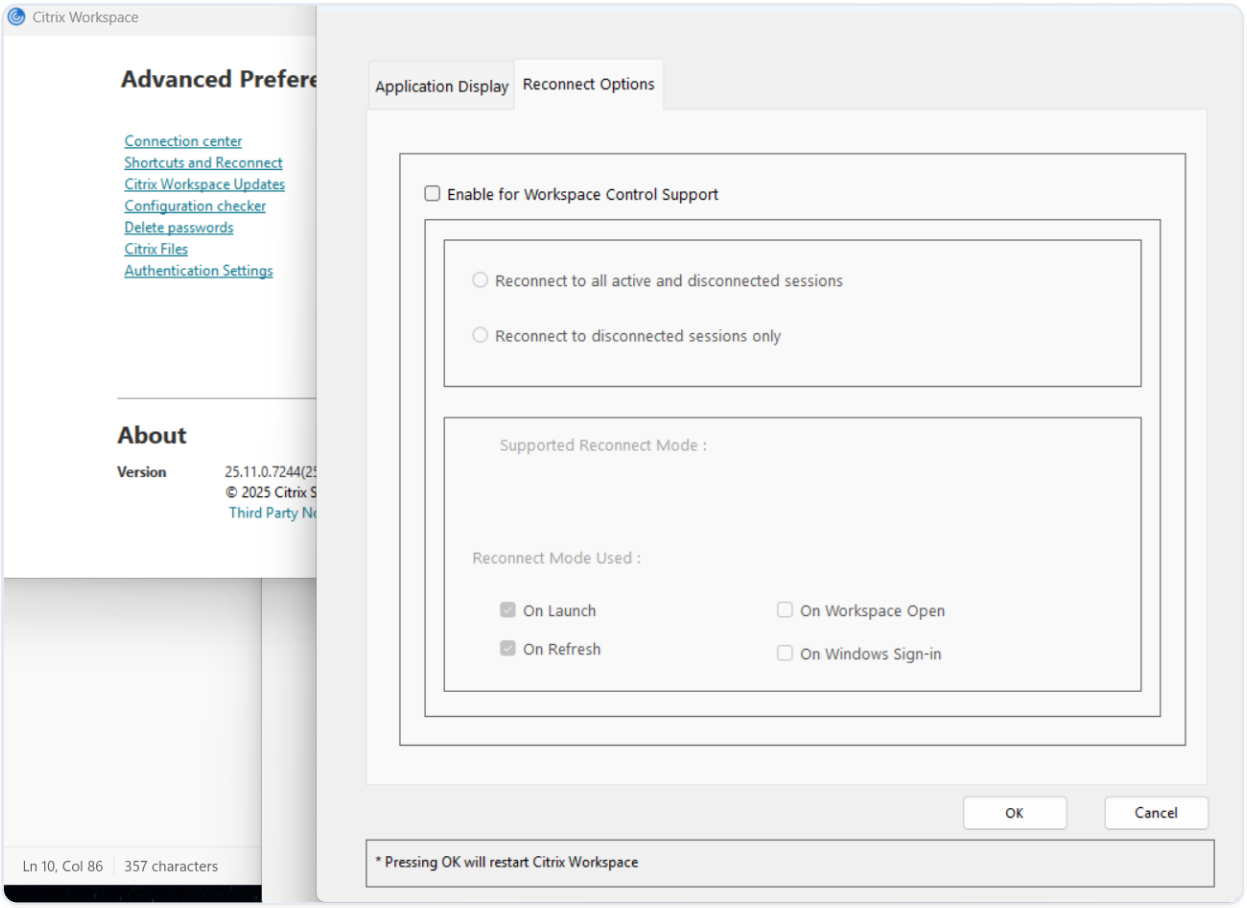


4. Enter the published resource name in the **Configured AppName** field.
5. Enter the **Max Launch Retries** from the drop-down list.
6. Select the **Enabled** checkbox.
7. Click **OK** and then click **Apply**.
8. Restart Citrix Workspace app for the changes to take effect.

When the Persistent ICA policy is enabled, administrators must disable Citrix Workspace reconnect to existing sessions. Administrators can disable Workspace Control using either the UI or Registry Editor.

To disable Workspace Control by using the UI:

1. Go to **Advanced Preferences** > **Shortcut and Reconnect** > **Reconnect Options**.
2. Clear the **Enable for Workspace Control Support** check box.



To disable Workspace Control by using Registry Editor:

1. Open Registry Editor.
2. Navigate to one of the following locations:
   - 64-bit systems: `Computer\HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\Citrix\Dazzle`
   - 32-bit systems: `HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\Dazzle`
3. Create a registry entry with the following values:
   - Type: `REG_SZ`
   - Name: `WSCSupported`
   - Value: `False`

Hybrid launch support using GACS for on-premises stores

Starting with version 2503, Citrix Workspace app for Windows supports management using Global App Configuration Service (GACS) in hybrid launch for on-premises stores. In a hybrid launch scenario, users access Citrix resources through a web browser. When an application or desktop is

selected, Citrix StoreFront™ generates an ICA file with the necessary launch instructions. The locally installed Citrix Workspace app then reads the ICA file, and establishes a secure connection to the remote application or desktop.

Key behavior:

- When a user launches a session, in-session settings apply from the next launch.
- If a store is added in the app and later accessed using a browser, settings are retrieved from the client app.
- Only the most recently accessed store applies its settings to the native app.

For example:

If a user first launches a session from one store, the app fetches and applies its GACS policies. Later, if the user switches to another store and launches a session, the app updates and applies the new store's GACS policies. For more information, see GACS supports hybrid launch.

Citrix Workspace app Desktop Lock

Overview

The Citrix Workspace app Desktop Lock, also known as direct boot to VDI, simplifies access to virtual desktops. This feature allows admins to configure local desktops so that users can directly access their virtual desktops without access to local resources or applications on the endpoint device.

Direct boot to VDI or Desktop Lock is ideal where data protection, compliance, and simplicity are top priorities for organizations. This solution locks users out of the endpoint operating system, keeping your data secure and reducing risk. It is ideal for the kiosk mode and frontline use cases.

Starting from Citrix Workspace app for Windows version 2503, the Citrix Workspace app Desktop Lock, includes the following enhancements:

- **Integrated installer**: Desktop Lock is now part of the main Citrix Workspace™ app installer, simplifying deployment and distribution for admins. When you install Citrix Workspace app using:
    - **Command line installation**: You can enable Desktop Lock using command-line parameters during the installation.
    - **UI**: You can enable Desktop Lock using the Group Policy Object (GPO) policy after the installation.

  You need to reboot the machine after enabling the Desktop Lock feature.
- **De-coupled from SSON**: Previously, you had to install the Citrix Workspace app for Windows with the `/includeSSON` flag to enable the Desktop Lock feature. Desktop Lock is now available without single sign-on (SSON). However, it is recommended to use it with SSON enabled for a seamless experience.
- **Enable feature through policy or command line**: You can manage the feature enablement through GPOs or command line. This enhancement provides granular controls to enable the feature at any point in time. The following policies can be managed in the Group Policy Editor:

  - **AllowDesktopLockOnMachine**: This policy is a machine-level policy that allows the ability to switch to Desktop Lock for any user on the machine. This policy requires a reboot of the machine.
  - **EnableDesktopLockforAllStandardUsers**: This policy is a machine-level policy that enables Desktop Lock for all standard users on the machine. Along with this policy, you need to enable the **AllowDesktopLockOnMachine** policy.
  - **EnableDesktopLockforUser**: This policy is a user group policy to enable or disable Desktop Lock for a specific user. Along with this policy, you need to enable the **AllowDesktopLockOnMachine** policy.

- **Post-installation configuration**: Stores can be configured post-installation, extending Desktop Lock to existing stores configured through GPO.
- **Support for Any Identity Provider (IDP)**: Desktop Lock now supports booting into VDI with any IdP that supports Citrix Workspace app.

Key features

- **Direct Virtual Desktop access**: Users land directly in their virtual desktop after logging into the local desktop.
- **Single sign-on (SSO) integration**: When single sign-on is enabled, users experience a seamless login process without needing to enter credentials multiple times. This integration is supported only with domain-joined endpoints.
- **Non-domain-joined machine support**: While primarily intended for domain-joined environments, Desktop Lock also supports user authentication on non-domain-joined machines. However, manual authentication is required in this scenario.
- **Flexibility**: Desktop Lock supports both shared and dedicated local desktops, catering to various use cases like kiosks and frontline users.

Benefits

- **Easier installation and configuration**: Simplifies the deployment process for admins.
- **Reduced login times**: Provides a faster login experience for users.
- **Seamless boot into VDI**: Enhances the overall user experience with a smooth transition into the VDI environment.
- **Flexible management**: Allows admins to manage and configure Desktop Lock at any point in time through policies.

These enhancements make the Desktop Lock feature more flexible and easier to manage, providing a better experience for both admins and users.

Note:

- You must reboot the machine after upgrading Citrix Workspace app for Windows with the Desktop Lock feature for the changes to take effect.
- For optimal functionality, domain-joined endpoints are recommended.

Configuring Desktop Lock

You can manage the Desktop Lock feature enablement through Group Policy Object (GPO)s or command line.

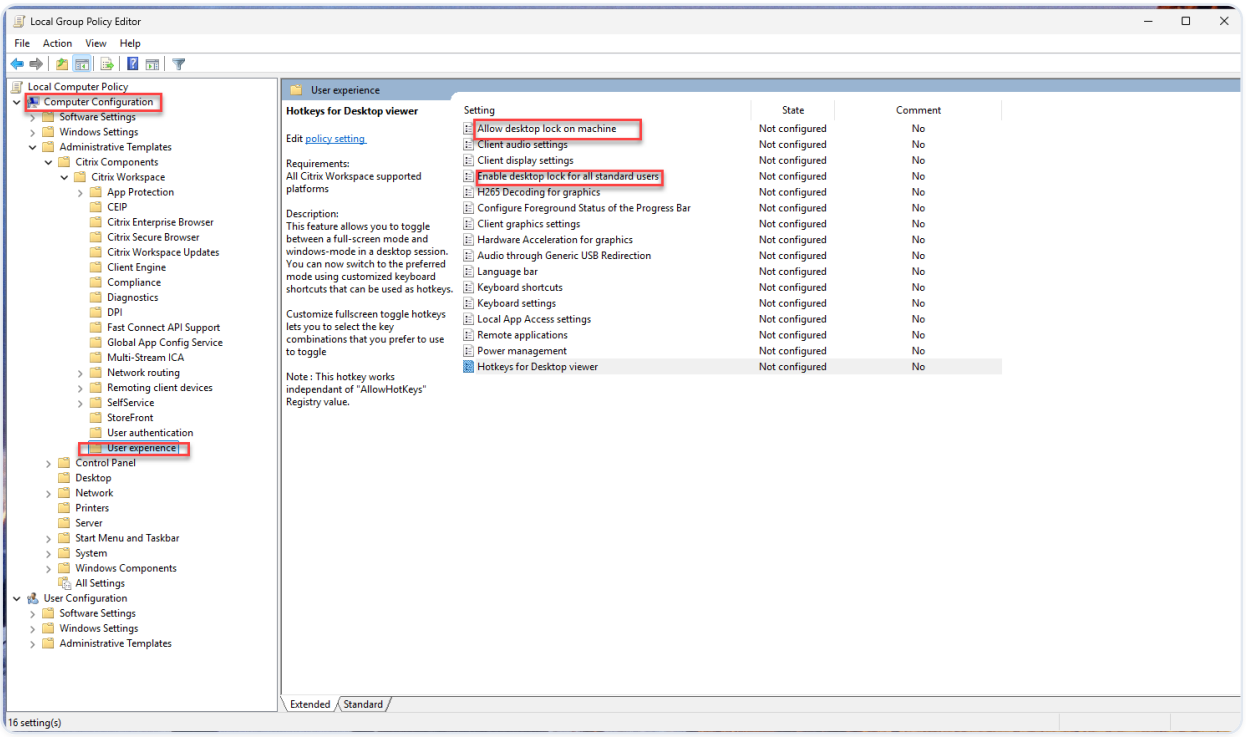
Enable Desktop Lock feature using GPO

You can enable or disable the Desktop Lock feature using Group Policy Object (GPO) for all standard users and specific sets of users. These specific sets of users might include admins as well.

Configuring Desktop Lock for all standard users

Perform the following steps to enable the feature using GPO:

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



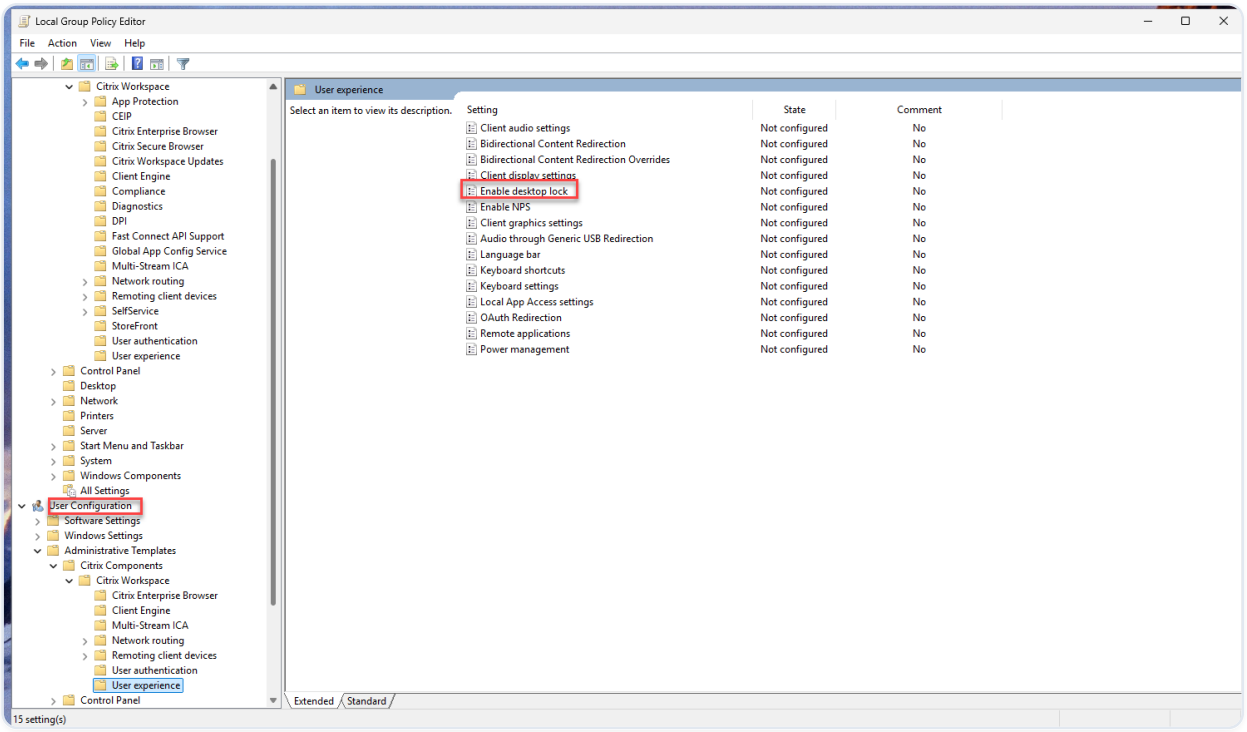
3. Select the **Allow desktop lock on machine** policy.
4. Select the **Enabled** checkbox.
5. Select the **Enable desktop lock for all standard users** policy.
6. Select the **Enabled** checkbox.
7. Click **OK** and then click **Apply**.
8. Reboot the machine.

Configuring Desktop Lock for specific users

Perform the following steps to enable the feature using GPO:

1. Open the Citrix Workspace app Group Policy Object administrative template by running **gpedit.msc** and navigate to the **Computer Configuration (local machine)** node.
2. Go to **Administrative Templates > Citrix Components > Citrix Workspace > User Experience**.
3. Select the **Allow desktop lock on machine** policy.
4. Select the **Enabled** checkbox.
5. Open the Citrix Workspace app Group Policy Object administrative template by running **gpedit.msc** and navigate to the **User Configuration** node.
6. Go to **Administrative Templates > Citrix Components > Citrix Workspace > User Experience**.

7. Select the **Enable desktop lock** policy.



8. Select the **Enabled** checkbox.
9. Click **OK** and then click **Apply**.
10. Reboot the machine.

> **Note:**
>
> The **User Configuration** > **Enable desktop lock** policy takes precedence over the **Computer Configuration**> **Enable desktop lock for all standard users** policy in case of the Desktop Lock feature.

Enable Desktop Lock feature using command line parameters

You can enable the Desktop Lock feature for all standard users on the machine using the following command line parameter:

```
CitrixWorkspaceApp.exe AllowDesktopLockOnMachine
EnableDesktopLockForAllStandardUsers
```

Note:

- By default the Desktop Lock feature is disabled. On enabling, if you want to disable the Desktop Lock feature, you can use the **Allow desktop lock on machine** GPO policy.
- It is not possible to enable the desktop lock feature for a specific user using the command line.
- After the Desktop Lock feature configuration, you can configure the store. Use the ADM/ ADMX file or command-line options to configure the store. For more information on installation using Group policy, see the Group Policy documentation.

Command line installation example:

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

Important considerations

- **Automatic desktop selection**: When using Citrix Workspace app for Windows with Desktop Lock, a user is signed in to the first available desktop. Currently, there is no option to selectively choose which desktop the user must sign in.
- **Desktop-only support**: This feature currently supports only desktops, not applications.
- **User profiles**: A local user profile is created on the device upon login. Profile retention depends on your Profile Management settings.
- **Session disconnection**: Disconnecting the Desktop Lock session logs the user out of the device.
- **Local device Task Manager**: Access to the local device's Task Manager is restricted.
- **Streamlined Desktop Viewer**: The Desktop Viewer is optimized for Desktop Lock. It does not include Home, Restore, Maximize, and Display properties.

Authentication

Citrix Workspace app Desktop Lock supports all the authentication methods available in Citrix Workspace app. For more information, see Authentication.

Shared devices

In a shared device scenario, multiple users can use the same local machine. Upon logging in with their designated authentication method to the local machine, users directly access the virtual desktop. Once signed out of the virtual desktop, the local device is immediately available for the next user. This setup is beneficial for organizations with shift workers or shared desktop environments.

Dedicated devices

In a dedicated device setup, a single user is assigned to the local machine. The virtual desktop opens directly upon login to the local machine using the assigned authentication credentials.

Additional supported features

- **HDX and Multimedia**: All HDX and multimedia features are supported. For more information, see HDX and multimedia.
- **Local App Access**: Local App Access is supported but requires careful configuration to prevent unauthorized access to the local desktop. For more information, see the Configure Local App Access and URL redirection section in the Citrix Virtual Apps and Desktops documentation.

Passing Windows shortcut keys to the remote session

Passing Windows shortcut keys to the remote session is supported with Desktop lock mode. For more information, see Passing Windows shortcut keys to the remote session.

Uninstalling Desktop Lock

The Desktop Lock feature is installed as part of the Citrix Workspace app. Therefore, uninstalling the Citrix Workspace app also removes the Desktop Lock feature. For more information, see Uninstall Citrix Workspace app

Software Development Kit (SDK) and API

Certificate Identity Declaration SDK

The Certificate Identity Declaration (CID) SDK lets developers create a plug-in. The plug-in lets Citrix Workspace app authenticate to the StoreFront server by using the certificate that is installed on the client machine. CID declares the user's smart card identity to a StoreFront server without performing a smart card-based authentication.

The latest version for Certificate Identity Declaration for Citrix Workspace for Windows is **2212**.

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 a set of native APIs that enables you to interact and perform basic operations programmatically. This SDK does not require a separate download because it is a part of the Citrix Workspace app for Windows installation package.

> **Note:**

> Some of the APIs that are related to launch require the ICA® file to initiate the launch process to virtual apps and desktops sessions.

> The CCM SDK capabilities include:

- Session launch
  - Allows launching applications and desktops using the generated ICA file.
- Session disconnect
  - Similar to the disconnect operation using the Connection Center. The disconnect can be for all the sessions or to a specific user.

- Session logoff
  - Similar to the logoff operation using the Connection Center. The logoff can be for all the sessions or to a specific user.
- Session information
  - Provides different methods to get connection-related information of the sessions launched. The session includes desktop session, application session, and reverse seamless application session

For more information about the SDK documentation, see Programmers guide to Citrix CCM SDK.

Citrix Virtual Channel SDK

The Citrix Virtual Channel software development kit (SDK) supports writing server-side applications and client-side drivers for more virtual channels using the ICA protocol. The server-side virtual channel applications are on Citrix Virtual Apps and Desktops™ servers. If you want to write virtual drivers for other client platforms, contact Citrix Technical support.

The Virtual Channel SDK provides:

- The Citrix Virtual Driver Application Programming Interface (VDAPI) is used with the virtual channel functions in the Citrix Server API SDK (WFAPI SDK) to create new virtual channels. The virtual channel support provided by VDAPI makes it easy to write your own virtual channels.
- 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.

The latest version for Virtual Channel SDK for Windows is **2302**.

For more information, see Citrix Virtual Channel SDK for Citrix Workspace app for Windows documentation.

Fast Connect 3 Credential Insertion API

The Fast Connect 3 Credential Insertion API provides an interface that supplies user credentials to the single sign-on (SSON) feature. This feature is available in Citrix Workspace app for Windows Version 4.2 and later. With this API, Citrix partners can provide authentication and SSO products that use StoreFront to log users on to virtual applications or desktops and then disconnect users from those sessions.

The latest version for Fast Connect API for Citrix Workspace for Windows is **2212**.

For more information, see Fast Connect 3 Credential Insertion API for Citrix Workspace app for Windows documentation.

Scripts for deploying Citrix Workspace for Windows

These are sample scripts to deploy and configure Citrix Workspace app.

The latest version for Scripts for deploying Citrix Workspace for Windows is **2212**.

Storebrowse

> **Note:**
>
> This article is applicable to on-premises deployments of Citrix Workspace only. For cloud deployements, see Storebrowse for Workspace documentation.

> **Storebrowse** is a command-line utility that interacts between the client and the server. It's used to authenticate all the operations within StoreFront and with Citrix Gateway.

Using the **Storebrowse** utility, administrators can automate the following operations:

- Add a store.
- List the published apps and desktops from a configured store.
- Generate an ICA® file by selecting any published virtual apps and desktops manually.
- Generate an ICA file using the **Storebrowse** command line.
- Launch the published application.

The **Storebrowse** utility is a part of the `Authmanager` component. When Citrix Workspace app installation is complete, the **Storebrowse** utility is in the `AuthManager` installation folder.

To confirm that the **Storebrowse** utility is installed along with the `Authmanager` component, check the following registry path:

When Citrix Workspace app is installed by administrators:

On a 32-bit machine	[HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\AuthManager\Install]
On a 64-bit machine	[HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\Citrix\AuthManager\Install]

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

On a 32-bit machine	[HKEY_CURRENT_USER\SOFTWARE\Citrix\AuthManager\Install]
On a 64-bit machine	[HKEY_CURRENT_USER\SOFTWARE\WOW6432Node\Citrix\AuthManager\Install]

Requirements

- Citrix Workspace app Version 1808 for Windows or later.
- Minimum of 530 MB of free disk space.
- 2 GB RAM.

Compatibility Matrix

Storebrowse utility is compatible with the following Operating systems:

OPERATING SYSTEM
Windows 10 32-bit and 64-bit editions
Windows Server 2022
Windows Server 2016

OPERATING SYSTEM
Windows Server 2008 R2, 64-bit edition
Windows Server 2008 R2, 64-bit edition

Connections

Storebrowse utility supports the following types of connections:

- HTTP store
- HTTPS store
- Citrix Gateway 11.0 and later

> **Note:**
>
> On an HTTP store, the **Storebrowse** utility does not accept credentials using the command-line.

Authentication methods

StoreFront servers

StoreFront supports different authentication methods to access stores, however, not all are recommended. For security purposes, some of the authentication methods are disabled by default while creating a store.

- **Username and Password**: Enter the credentials to be authenticated to access stores. By default, Explicit authentication is enabled when you create your first store.
- **Domain Pass-through**: After authenticating to the domain-joined windows computers, you're automatically logged on to stores. To use this option, enable pass-through authentication when installing the Citrix Workspace app. For more information on domain pass-through, see Configuring Pass-through authentication.
- **HTTP Basic**: This method is used by third-party client integrations and web portals, where an external user interface has been used to capture a domain-qualified user name and password. StoreFront uses the Basic Authentication feature in IIS to transport the credentials to the StoreFront server. StoreFront then uses either the Domain Services, or the Broker XML Service authentication to validate the credentials and to obtain the group information. For information

on how to enable HTTP Basic authentication, see HTTP Basic in the Manage authentication methods documentation.

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

- Using the `AuthManager` that is in-built along with the **Storebrowse** utility. Note: Enable the HTTP Basic authentication method on the StoreFront while working with the **Storebrowse** utility. This method applies when the user provides the credentials using the **Storebrowse** commands.
- Use the `Authmanager` that is included with Citrix Workspace app for Windows. You can use this method, when you use domain pass-through authentication. For more information, see Domain pass-through authentication documentation.

Launch published desktop or application

You can now launch a resource directly from the store without having to use an ICA file.

> **Note:**
>
> You can't open SaaS apps or published content using Storebrowse commands.

Command usage

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

Add a store

`-a`, `--addstore`

Description:

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

> **Note:**
>
> Multi-store configuration is supported on the **Storebrowse** utility.

> **Command example on StoreFront:**

Command:

```
storebrowse.exe –U *username* -P *password* -D *domain* -a *URL of StoreFront*
```

Example:

```
.\storebrowse.exe –U {Username} –P {Password} –D {Domain} –a [https://my.firstexamplestore.net](https://my.firstexamplestore.net)
```

Command example on Citrix Gateway:

Command:

```
storebrowse.exe –U *username* -P *password* -D *domain* -a *URL of CitrixGateway*
```

Example:

```
.\storebrowse.exe –U {Username} –P {Password} –D {Domain} –a <https://mysecondexample.com>
```

The above will work if the StoreFront configured with gateway has a single store.

If the StoreFront configured with gateway has multiple stores, the following command needs to be used:

Command: `storebrowse.exe –U *username* -P *password* -D *domain* -a *URL of CitrixGateway*?StoreName`

Example: `.\storebrowse.exe –U {Username} –P {Password} –D {Domain} –a https://mysecondexample.com?Store`

Help

`/?`

Description:

Provides details on **Storebrowse** utility usage.

List store

`(-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
```

Enumerate

`(-M 0x2000 -E)`

Description:

Enumerates 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.secondexample.net>
```

Quick launch

`-q`, `--quicklaunch`

Description:

Generates the ICA file for published apps and desktops using the **Storebrowse** utility. The `quicklaunch` option requires a launch URL as an input along with the Store URL. The launch URL which can either be the StoreFront server or the Citrix Gateway URL. The ICA file is generated in the `%LocalAppData%\Citrix\Storebrowse\cache` directory.

You can get the launch URL for any published apps and desktops by running the following command:

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

A typical launch URL is as follows:

`'Controller.Calculator' 'Calculator' '\' '' http://abc-sf.xyz.com/Citrix/Stress/resources/v2/Q29udHJvbGxlci5DYWxjdWxhdG9y/launch/ica`

Command example on StoreFront:

`.\storebrowse.exe –U {Username} –P {Password}–D {Domain} –q {Launch_URL_of_published_ apps and desktops }` https://my.firstexamplestore.net/Citrix/Store/resources/v2/Q2hJkOlmNoPQrSTV9y/launch/ica `<https://my.firstexamplestore.net/Citrix/Store/discovery>`

Command example on Citrix Gateway:

`.\storebrowse.exe –U {Username} –P {Password} –D {Domain} –q {Launch_URL_of_published_ apps and desktops} <https://my.secondexmaplestore.com>`

Launch

`-L`, `--launch`

Description:

Generates the required ICA file for published apps and desktops using the **Storebrowse** utility. The launch option requires the name of the resource along with the Store URL. The name which can either be the StoreFront server or the Citrix Gateway URL. The ICA file is generated in the `%LocalAppData%\Citrix\Storebrowse\cache` directory.

Run the following command to get the display name of the published apps and desktops:

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

This command results in the following output:

`'Controller.Calculator' 'Calculator' '\' '' http://abc-sf.xyz.com/Citrix/Stress/resources/v2/Q29udHJvbGxlci5DYWxjdWxhdG9y/launch/ica`

Command example on StoreFront:

`.\storebrowse.exe -U {Username} –P {Password} –D {Domain} –L “{Resource_Name} <https://my.firstexamplestore.net/Citrix/Store/discovery>`

Command example on Citrix Gateway:

`<.\storebrowse.exe –U {Username} –P {Password} –D {Domain} –L {Resource_Name} https://my.secondexamplestore.com>`

Session launch

`-S`, `--sessionlaunch`

Description:

With this command, you can add a store, verify, and launch the published resources. This option takes the following as parameters:

- User name
- Password
- Domain
- Name of the resource to be launched
- Store URL

However, if the user does not provide the credentials, the `AuthManager` prompts to enter the credentials and then the resource is launched.

You can get the name of the resource of published apps and desktops by running the following command:

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

This command results in the following output:

`'Controller.Calculator' 'Calculator' '\' '' http://abc-sf.xyz.com/Citrix/Stress/resources/v2/Q29udHJvbGxlci5DYWxjdWxhdG9y/launch/ica`

The name that is in bold in the previous output is used as the input parameter to the `-S` option.

Command example on StoreFront:

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

Command example on Citrix Gateway:

```
.\storebrowse.exe –U {Username} –P {Password} –D {Domain} –S {Friendly_Resource_Name} <https://my.secondexamplestore.com>
```

File folder

`-f`, `--filefolder`

Description:

Generates the ICA file in the custom path for the published apps and desktops.

The launch option requires a folder name and the name of the resource as the input with the Store URL. The Store URL can either be the StoreFront server or the Citrix Gateway URL.

Command example on StoreFront:

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

Command example on the Citrix Gateway:

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

Trace authentication

`-t`, `--traceauthentication`

Description:

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

> **Note:**
>
> This option must not be the last parameter listed in the user's command line.

> Command example on StoreFront:

```
.\storebrowse.exe –t –U {UserName} –P {Password} –D {Domain} –a {StoreURL}
```

Command example on Citrix Gateway:

```
.\storebrowse.exe –t –U {UserName} –P {Password} –D {Domain} –a {NSG_URL}
```

Delete a store

`-d`, `--deletestore`

Description:

Deletes existing StoreFront or Citrix Gateway store.

Command example on StoreFront:

```
.\storebrowse.exe –d https://my.firstexamplestore.net/Citrix/Store/discovery
```

Command example on Citrix Gateway:

```
.\storebrowse.exe –d https://my.secondexmaplestore.com
```

Tracking Storebrowse command status

Starting with 2305.1 release, you can track the execution status of a Storebrowse command in a file. To track the success status, provide a unique file name with the `-f launch` command. This command generates a file with the name that you have provided. The failure status is present in the `ica.error` file, which is created automatically.

> **Note:**
>
> Ensure that you add an `.ica` extension to the file name with `-f launch` command. Otherwise, the file isn't generated.
>
> The files to track both success and failure are present at `%LOCALAPPDATA%\citrix\selfservice\cache` and you can monitor these files as needed.

This enhancement is enabled by default.

Following is an example to use the launch command with `-f` option:

```
-launch -f <uniqueFileName.ica> "launchcommandline"

For example:

SelfService.exe storebrowse -launch -f uniqueFileName.ica -s
```

```
store0-5c3ec017 -CitrixID store0-5c3ec017@@a9a8e3ac-099d-4577-b84e-
e33d0695df39.Notepad -ica "https://cwawiniwstest.cloudburrito.com/Citrix/
Store/resources/v2/
YTlhOGUzYWMtMDk5ZC00NTc3LWI4NGUtZTMzZDA2OTVkZjM5Lk5vdGVwYWQ-/launch/ica"
-cmdline
```

Single sign-on support with Citrix Gateway

Single sign-on lets you authenticate to a domain and use the Citrix Virtual Apps and Desktops™ and Citrix DaaS (formerly Citrix Virtual Apps and Desktops service)that the domain provides. You can sign in without having to reauthenticate to each app or desktop. When you add a store, your credentials pass through the Citrix Gateway server, along with the Citrix Virtual Apps and Desktops and Citrix DaaS, and Start menu settings.

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

Prerequisites:

For the prerequisites on how to configure Single Sign-On for the Citrix Gateway, see Configure domain pass-through authentication.

The single sign-on feature with Citrix Gateway can be enabled using the Group Policy Object (GPO) administrative template.

1. Open the Citrix Workspace app GPO administrative template by running gpedit.msc
2. Under the **Computer Configuration node**, go to **Administrative Template** > **Citrix Component** > **Citrix Workspace** > **User Authentication** > **Single Sign-on for Citrix Gateway**.
3. Use the toggle options to Enable or Disable the Single Sign-On option.
4. Click **Apply** and **OK**.
5. Restart the Citrix Workspace app session for the changes to take effect.

Limitations:

- Enable the **HTTP Basic Authentication** method on the StoreFront server for credential injection operations with the **Storebrowse** utility.
- If you have an HTTP store and try to connect to the store using the utility to check or launch the published virtual apps and desktops, the credential injection using the command-line option is

unsupported. As a workaround, use the external `AuthManager` module if you do not provide credential using the command line.

- **Storebrowse** utility currently supports only single store configured the Citrix Gateway on the StoreFront server.
- Credential Injection in the **Storebrowse** utility works only if the Citrix Gateway is configured with Single-Factor Authentication.
- The command-line options `Username (-U)`, `Password (-P`) and `Domain (-D)` of the **Storebrowse** utility are case-sensitive and must be in upper case only.

To enable SSON for third-party applications that uses ICOSDK, create the following registry:

- Registry Key: `Computer\HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\Citrix\ICA Client\NonIEAppsWithSson`
- Registry Value: full path of the third-party applications
- Registry Type: reg_multi_sz

Example:

- Registry Key: `Computer\HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\Citrix\ICA Client\NonIEAppsWithSson`
- Registry Value: C:\temp1\abc.exe;C:\temp2\xyz.exe
- Registry Type: reg_multi_sz

Note:

- You can provide multiple third-party applications separated by semicolon.
- This feature is supported on Version 2107 onwards.

Enhanced storebrowse session handling

Starting with this release, storebrowse' session handling is improved with the following enhancements, optimizing user experience and critical resource management within high-availability environments to boost efficiency:

- **Storebrowse intelligently ignores existing sessions when launching virtual applications** - This option prevents reconnects to sessions actively being torn down by the system now, improving stability. This ensures seamless, error-free access to critical business applications,

especially during client updates, simplifying management by reducing complex configuration needs. To enable intelligent session handling, administrators must add the -I true parameter to existing storebrowse commands. This parameter integrates seamlessly with all existing launch types while maintaining current syntax structure.

Command example:

Quick Launch:

Previous syntax:

```
.\storebrowse.exe -U {Username} -P {Password} –D {Domain} -q
{Launch_URL_of_published_ apps and desktops} <https://cwa-
ddc2c.cwa.com/Citrix/Store/resources/v2/
Q29udHJvbGxlci5DYWxjdWxhdG9yLVRTVkRBMTk-/launch/ica> < https://cwa-
ddc2c.cwa.com/citrix/store/discovery>
```

Enhanced syntax with intelligent session handling:

```
.\storebrowse.exe -U {Username} -P {Password} –D {Domain} -I true -q
{Launch_URL_of_published_ apps and desktops} https://cwa-ddc2c.cwa.com/
Citrix/Store/resources/v2/Q29udHJvbGxlci5DYWxjdWxhdG9yLVRTVkRBMTk-/
launch/ica> < https://cwa-ddc2c.cwa.com/citrix/store/discovery>
```

- **Storebrowse API support for returning session lists** - This option provides valuable visibility into active user sessions, enabling more contextualized and efficient session launches. This improved visibility decreases user-impacting errors and delays during application access, ensuring a smoother, more reliable experience for all users.

Storebrowse for Workspace

Citrix Workspace app for Windows provides **Storebrowse** support on self-service and on-premises deployment of Citrix Workspace app. It also enables **Storebrowse** users to access Cloud and Workspace features.

> **Note:**

- This article is applicable to cloud deployments of Citrix Workspace only. For on-premises deployements, see Storebrowse documentation.
- This feature provides **Storebrowse** support with single sign-on only.
- The prerequisites mentioned in System requirements and compatibility must be available to use this feature.
- You can't open SaaS apps or published content using Storebrowse commands.

Command usage

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

Note:

- This feature also supports other self-service plug-in commands as mentioned in the CTX200337.
- You can execute the following commands in the command prompt.

- `-a "discoveryurl"`: Adds a store via command line. This command doesn't show the Authentication prompt where SSO is enabled. For example, AAD domains join devices where authentication happens through webview. On other devices, the Authentication prompt appears.
  - Example: `SelfService.exe storebrowse -a "https://cwawiniwstest.cloudburrito.com/citrix/store/discovery"`
- `-d "discoveryurl"`: Deletes the store.
  - Example: `SelfService.exe storebrowse -d "https://cwawiniwstest.cloudburrito.com/citrix/store/discovery"`
- `-e "discoveryurl"`: Exports the resource details in the JSON format. This command stores the resource.json file in the `%LOCALAPPDATA%\citrix\selfservice` default location. Citrix Workspace app must be active to run this command and user must be signed in.

  - Example: `SelfService.exe storebrowse -e "https://cwawiniwstest.cloudburrito.com/citrix/store/discovery"`

  You can also specify your own path if you don't want to store the resource.json in the default location.

  - Example: `.\SelfService.exe storebrowse -e "https://cwawiniwstest.cloudburrito.com/citrix/store/discovery" "C:\Users\<username>\Documents\Fiddler2"`. This stores the resource.json file in the `C:\Users\<username>\Documents\Fiddler2`.

- `-q "FriendlyName" "discoveryurl"`: Use this command to perform quick launch of the specified resource.

  - Example: `SelfService.exe storebrowse -q "Excel 2016" "https://cwawiniwstest.cloudburrito.com/citrix/store/discovery"`

- `-launch "launchcommandline"`: Launch of resources using "launchcommandline" from resource.json.

  > **Note:**
  >
  > - Copy the "launchcommandline" from the resource.json.
  > - Remove **/** from the "launchcommandline" specified in the resource.json file before executing the command.

  - Example: `SelfService.exe storebrowse -launch -s store0-5c3ec017 -CitrixID store0-5c3ec017@@a9a8e3ac-099d-4577-b84e-e33d0695df39.Notepad -ica "https://cwawiniwstest.cloudburrito.com/Citrix/Store/resources/v2/YTlhOGUzYWMtMDk5ZC00NTc3LWI4NGUtZTMzZDA2OTVkZjM5Lk5vdGVwYWQ-/launch/ica" -cmdline`

  After executing the `-launch "launchcommandline"`, the ica file will be stored in the `%LOCALAPPDATA%\citrix\selfservice\cache` directory. Double-click the ica file to launch the resource.

- `-liststore`: Lists the stores that are added inside SSP. Store list to include storeID, discovery url for each store.

- Example: `SelfService.exe storebrowse -liststore`

> **Note:**
>
> Citrix Workspace app must be active to execute the `-liststore` command.

> `Selfservice.exe storebrowse -liststore` command stores the storedetails.json file in the `AppData\Local\Citrix\SelfService`.

Troubleshoot

Log collection

Log collection simplifies the process of collecting logs for Citrix Workspace app. The logs help Citrix to troubleshoot, and, in cases of complicated issues, provides support. This feature is available from Citrix Workspace app for Windows 2012 version and later.

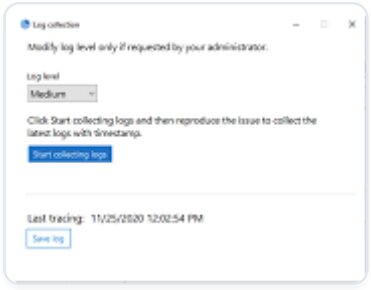
Note:

> Starting with the 2503 version of Citrix Workspace app complete log collection is possible for users for whom Citrix Workspace app is installed by an admin.

> You can collect logs using the GUI.

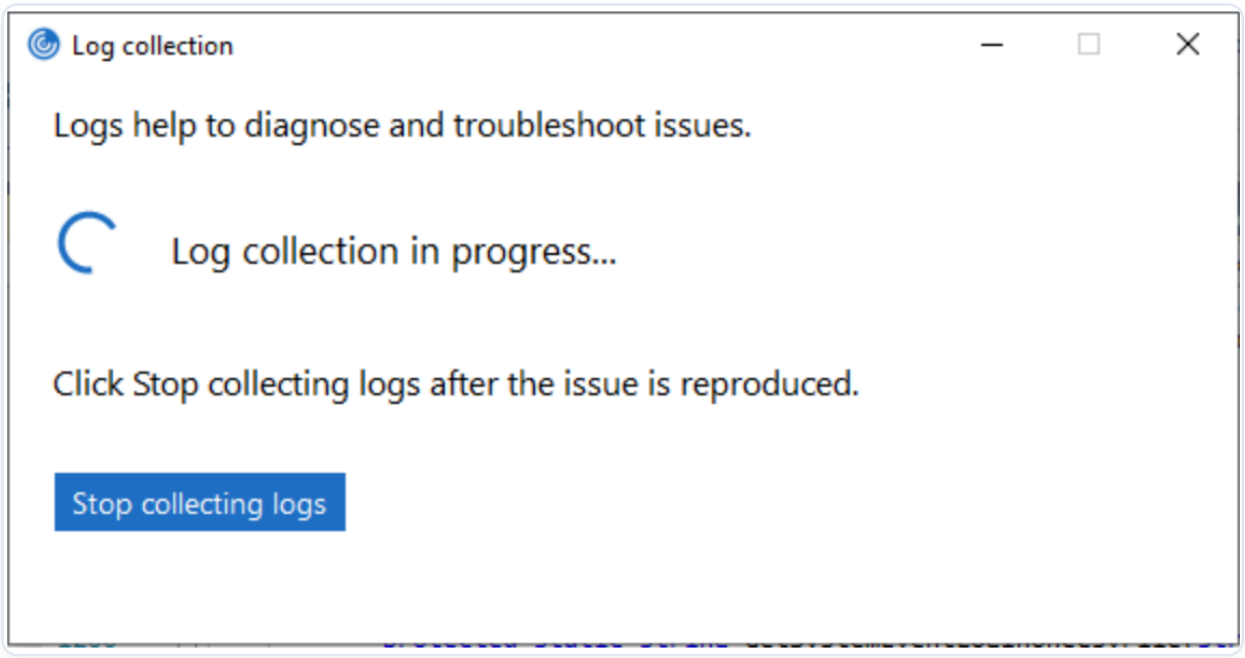
Collecting logs:

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



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

    The log collection process starts.



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

Data collected through logs

Hardware

- Attached monitors information
- Memory information
- Network adapters
- Processor
- Direct X diagnostics information

Software

- Citrix Workspace app version
- OS information (version, service pack, and architecture)
- Internet Explorer version
- Default browser
- ActiveX Flash version
- NPAPI Flash version

Registry

- HKEY_LOCAL_MACHINE\Software\Citrix\AuthManager
- HKEY_LOCAL_MACHINE\Software\Citrix\CitrixCAB
- HKEY_LOCAL_MACHINE\Software\Citrix\Dazzle
- HKEY_LOCAL_MACHINE\Software\Citrix\ICA Client
- HKEY_LOCAL_MACHINE\Software\Citrix\Install
- HKEY_LOCAL_MACHINE\Software\Citrix\InstallDetect
- HKEY_LOCAL_MACHINE\Software\Citrix\PluginPackages
- HKEY_LOCAL_MACHINE\Software\Citrix\Receiver
- HKEY_LOCAL_MACHINE\Software\Citrix\ReceiverInside
- HKEY_LOCAL_MACHINE\Software\Citrix\XenDesktop
- HKEY_LOCAL_MACHINE\Software\Policies\Citrix
- HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Internet Settings\Zones
- HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Internet Settings\ZoneMap\Domains
- HKEY_LOCAL_MACHINE\System\CurrentControlSet\Control\NetworkProvider\Order
- HKEY_CURRENT_USER\Software\Citrix\AuthManager
- HKEY_CURRENT_USER\Software\Citrix\CitrixCAB
- HKEY_CURRENT_USER\Software\Citrix\Dazzle
- HKEY_CURRENT_USER\Software\Citrix\ICA Client
- HKEY_CURRENT_USER\Software\Citrix\Install
- HKEY_CURRENT_USER\Software\Citrix\InstallDetect
- HKEY_CURRENT_USER\Software\Citrix\PluginPackages
- HKEY_CURRENT_USER\Software\Citrix\Receiver
- HKEY_CURRENT_USER\Software\Citrix\ReceiverInside
- HKEY_CURRENT_USER\Software\Citrix\XenDesktop
- HKEY_CURRENT_USER\Software\Policies\Citrix
- HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\VisualEffects
- HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Internet Settings\Zones

- HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Internet Settings\ZoneMap\Domains

Event Logs

- Application Event log
- System Event log

Tracing

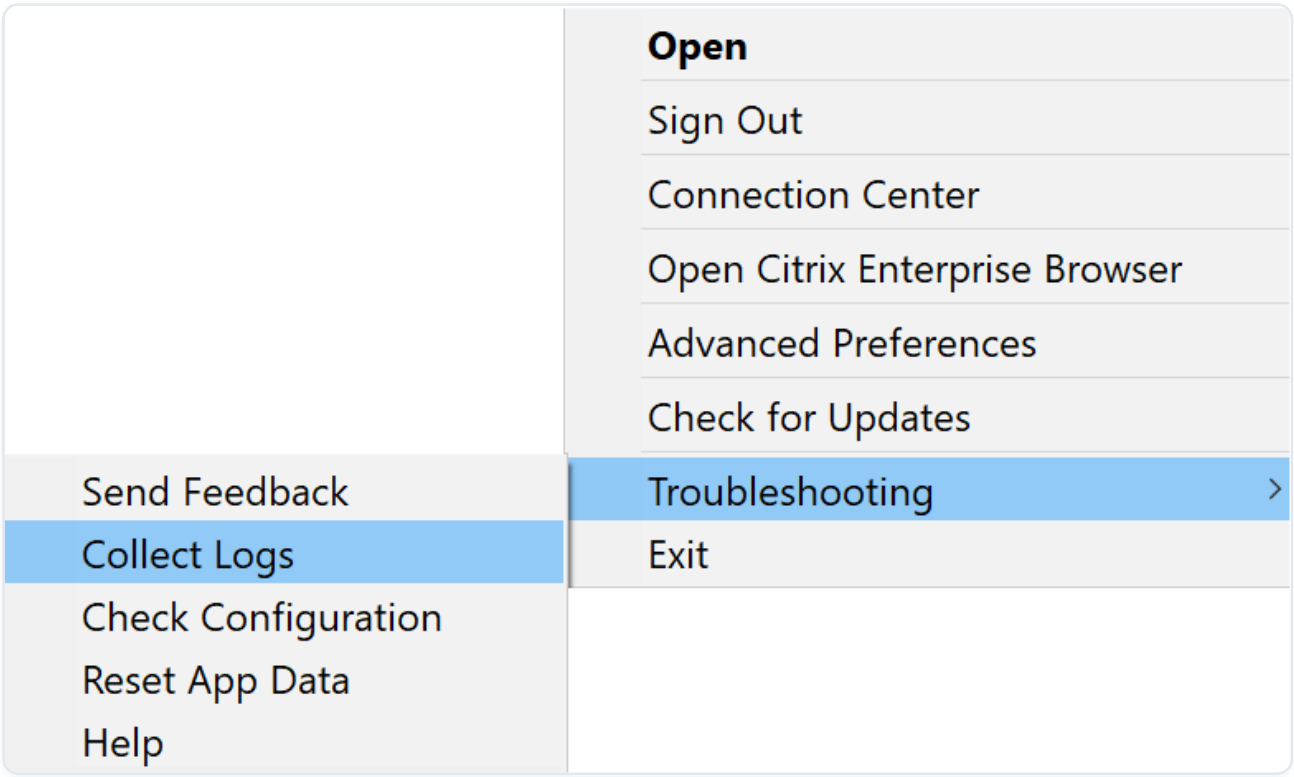
- HDX™
- Receiver shell, Auth Manager, and Self-Service plug-in
- Install logs
- Always-On logs

Addition of the Troubleshooting option in the system tray of Citrix Workspace app

From Citrix Workspace app 2309 version and later, the **Troubleshooting** option is introduced to improve the user experience and to easily proceed with the troubleshooting. You can right-click on the Citrix Workspace app icon in the system tray that is placed in the bottom-right corner of your screen and then select **Troubleshooting** to access it.

The options available under Troubleshooting are:

- Send Feedback
- Collect Logs
- Check Configuration
- Reset App Data
- Help

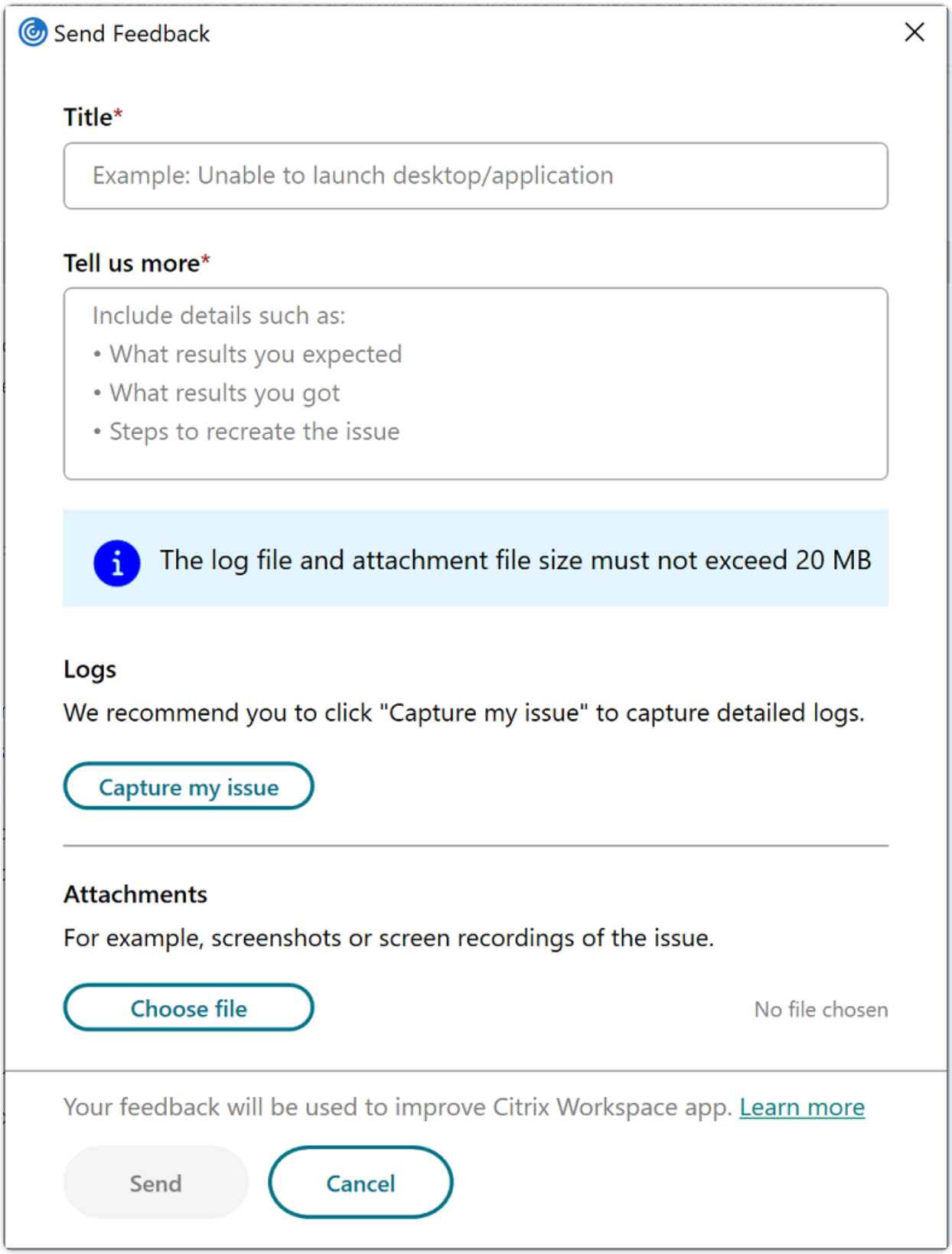


Send feedback on Citrix Workspace app

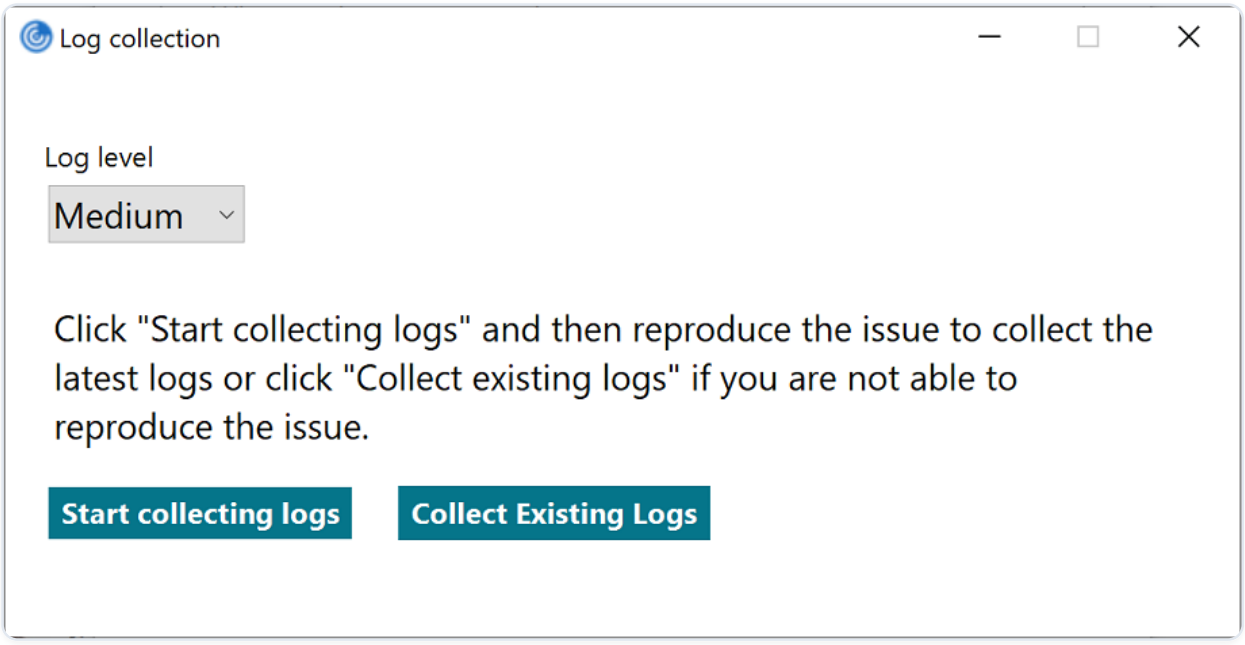
The **Send feedback** option allows you to inform Citrix about any issues that you might run into while using Citrix Workspace app. You can also send suggestions to help us improve your Citrix Workspace app experience.

You can submit feedback using the following steps:

1. Right-click the Citrix Workspace app icon in the notification area and select **Troubleshooting** > **Submit feedback**. The **Submit Feedback** screen appears.



2. Provide the issue **Title**.
3. Add issue details in the **Tell us more** field.
4. Click **Capture my issue**. The **Log collection** screen appears.



a. Click **Start collecting logs** and then reproduce the issue to collect the latest logs.

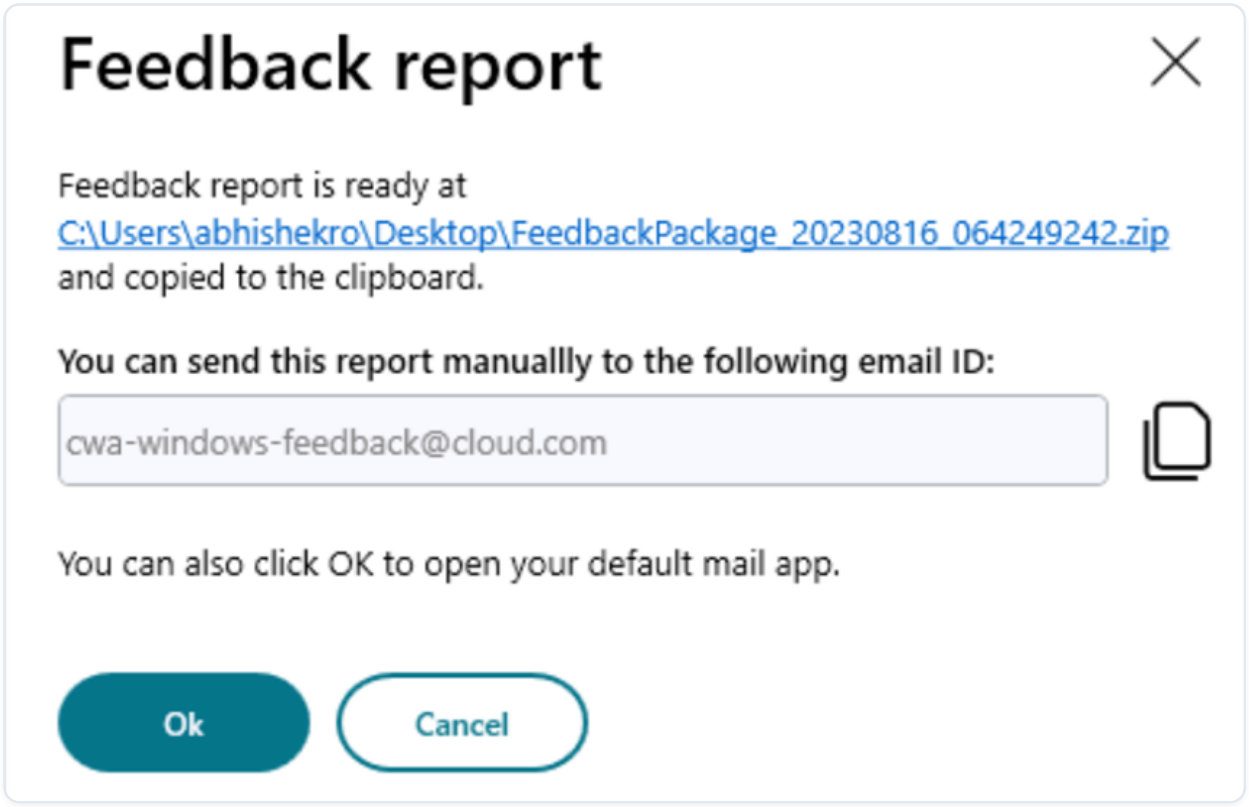
b. Click **Stop collecting logs** after the issue is reproduced.

   Or,

   Click **Collect existing logs** if you are not able to reproduce the issue.

c. Click **Stop collecting logs** after the issue is reproduced.

5. Ensure that the log files are displayed next to **Capture my issue**.
6. Click **Choose file** and then add attachments that describe your issues such as screenshots or screen recordings. The maximum file size allowed for all the attachments including the log file is 20 MB.
7. Click **Send**. The **Feedback report** screen appears.



The .zip file contains the log files, the issue description as test files, and the attachments.

8. You can send the feedback report to Citrix® using the following options:

- Click **Ok** to use the default mail app in your system.

Or,

- Send the report manually to the provided email ID.

> **Note:**
>
> Ensure that the .zip file is attached in the email.

ICA® file logging

When a user launches an app or desktop, StoreFront or Citrix Workspace generates an `ICA` file that Citrix Workspace app reads to determine how to connect to the app or desktop. Depending on the configuration, this file might be stored in memory and not directly accessible. To diagnose launch errors, it can be useful to view the contents of the `launch.ica` file.

To enable logging of the `launch.ica` file on the client PC, complete the following steps:

1. Navigate to the following registry key by using the registry editor:

32-bit Systems: `HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\ICA Client\Engine\Configuration\Advanced\Modules\Logging`

64-bit Systems: `HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Citrix\ICA Client\Engine\Configuration\Advanced\Modules\Logging`

2. Set the following two string key values:

   - LogFile="path to the log file"
   - LogICAFile=true

   For example:

```
LogFile=C:\ica\ica.log

LogICAFile=true
```

Citrix Troubleshoot Connection

Citrix empowers end users to self-troubleshoot desktop or app launch failures. The system provides recommendations to fix issues. Users can execute fixes with a single button click. Enhanced error messages help users understand launch failure causes clearly.

The Citrix Troubleshoot Connection feature analyzes VDA reachability challenges during launch. It provides user-friendly error messages in real time during failures. The feature offers recommendations to fix issues or collect logs for support tickets.

Potential virtual app and desktop launch issues

Launch issues can occur in these connection points:

- Network connectivity from Client to gateway
- Gateway to StoreFront™ server
- StoreFront server to Broker connection
- Broker to VDA connection

User-friendly error messages and diagnostics

Citrix displays clear, user-friendly error messages when launches fail. The messages point to specific connection issues. Examples include network errors, server unavailability, and VDA failures.

Self-recovery and recommendations

The Citrix Troubleshoot Connection feature includes steps for automatic recovery. This reduces support tickets. The following problems can be resolved with remediation:

- Restart VDA
- Restart CWA
- Re-Login To CWA
- Refresh Resource List
- Refresh App and try
- Reconfigure The Store
- Upgrade CWA
- Reinstall CWA
- Check Network
- Wait And Retry

System requirements

- Citrix Workspace app for Windows 2507.1 and later versions

Feature details

The Troubleshoot Connection feature is enabled by default for DaaS environments. Enhanced error messages and recommendations are provided for both browser-launched sessions and native Citrix Workspace app sessions.

Error codes are references for administrators and are available in logs. The codes are split between server-side errors and client-side errors. The feature provides "Restart VDA" as a remediation action for some errors. It does not support sessions launched through hybrid launch mode (downloading ICA file from browser and launching with native Citrix Workspace app).

Common server-side errors

ERROR ID	DESCRIPTION	RECOMMENDATION
ResourceNotFound	The resource was removed by your administrator.	For an up-to-date list of available apps and desktops, either refresh Citrix

ERROR ID	DESCRIPTION	RECOMMENDATION
		Workspace app or log out and back in.
WorkstationInMaintenance	The desktop is under planned maintenance.	Wait until the maintenance is complete, then try again.
UnavailableDesktop	There are no desktops available to connect to.	Wait a few minutes, then try again. If the issue persists, contact your system administrator.
UnavailableAppProtectedDesktop	App Protection required to open resources.	Upgrade to a Citrix Workspace app version with App Protection, or contact your system administrator for assistance.
NotLicensed	Unable to launch the resource because the server is missing the appropriate license.	Contact your system administrator for assistance.
NoMoreActiveSessions	Unable to launch the resource because there are no available session slots.	Wait a few minutes, then try again. If the issue persists, contact your system administrator.
GeneralAppLaunchError	An unknown error occurred while trying to open the resource.	Contact your system administrator for assistance.
ResourceDisabled	The resource was disabled by your administrator.	For an up-to-date list of available apps and desktops, either refresh Citrix Workspace app or log out and back in.

Citrix Workspace app for Windows errors

ERROR ID	DESCRIPTION	RECOMMENDATION
CertificateError	An error occurred with the server certificate.	Contact your system administrator for assistance.
PassthroughClientError	There is already an active session.	Contact your system administrator for assistance.
IcaFileRetrieveError	An error occurred while trying to retrieve the ICA file.	Contact your system administrator for assistance.
Icafileretrieveerrorreconnection	An error occurred while trying to retrieve the ICA file during reconnection.	Contact your system administrator for assistance.
NoCWA	Citrix Workspace app required to open resources.	Install Citrix Workspace app or contact your system administrator for assistance.
CouldNotFindStore	Unable to retrieve the required store configuration to launch the resource.	Remove the store from Citrix Workspace, then add it again. If the issue persists, contact your system administrator.
noclientinstalled	Unable to retrieve the required information to launch the resource.	Refresh Citrix Workspace app or log out and back in.
AuthCancelled	The authentication session expired.	To try to resolve the issue, reauthenticate in Citrix Workspace. If the issue persists, contact your system administrator.
IcaFileLaunchError	An error occurred while trying to start the ICA file.	Quit and reopen Citrix Workspace. If the issue persists, contact your system administrator.
CouldNotContactStore	An error occurred while trying to communicate with the	Quit and reopen Citrix Workspace. If the issue

ERROR ID	DESCRIPTION	RECOMMENDATION
	VDA. This could be due to a server connection issue.	persists, contact your system administrator.
CCMError	Unable to launch the resource due to a Connection Manager error. Error code: {errorCodeValue}	Quit and reopen Citrix Workspace. If the issue persists, contact your system administrator.
CCMInitFailed	Unable to launch the resource because the Connection Manager failed to initialize.	Quit and reopen Citrix Workspace. If the issue persists, contact your system administrator.
CCMLoadFailed	Unable to launch the resource because the Connection Manager failed to load.	Quit and reopen Citrix Workspace. If the issue persists, contact your system administrator.
InvalidIcaParams	Unable to launch the resource due to incorrect ICA parameters.	Quit and reopen Citrix Workspace. If the issue persists, contact your system administrator.
AppExiting	Unable to launch the resource because the Citrix Workspace app is exiting.	Quit and reopen Citrix Workspace. If the issue persists, contact your system administrator.
UTF8ConversionFailed	Unable to parse the ICA file.	Quit and reopen Citrix Workspace. If the issue persists, contact your system administrator.
MissingSoftware	You need additional software to use this app.	Contact your system administrator for assistance.

Deprecation

The announcements in this article give you advanced notice of platforms, Citrix® products, and features that are being phased out. Using these announcements, you can make timely business decisions.

Citrix monitors customer use and feedback to determine when they're withdrawn. Announcements can change in subsequent releases and might not include every deprecated feature or functionality.

Deprecated items aren't removed immediately. Citrix continues to support them in this release but they'll be removed in the future.

Deprecation table

ITEM	DEPRECATION ANNOUNCED IN	REMOVED IN	ALTERNATIVE
TLS 1.1 and 1.0	2409	2409	TLS 1.2 or TLS 1.3
Domain pass-through authentication	2405		Use enhanced domain pass-through for single sign-on.
Support for Windows Server 2016	2405	2405	Use the supported operating system as given in the System requirements section.
Citrix Ready® workspace hub (also known as WorkspaceHub)	2402	2402	
XenApp® Services (also known as PNAgent)	2403	2409	Within workspace app, connect to stores using the

ITEM	DEPRECATION ANNOUNCED IN	REMOVED IN	ALTERNATIVE
			store URL rather than the XenApp Services URL
Internet Explorer-based browser content redirection	2311.1	2311.1	Google Chrome based browser content redirection
Support for WebRTC SDP format (Plan B)	2309		Upgrade Citrix Workspace app to a supported version.
Support for Single Window mode in Microsoft Teams Optimization	2309		Upgrade Citrix Workspace app to a version that supports MultiWindow mode. For more information, see Feature matrix and version support.
`/includeappprotection` switch	2212	2212	Use `/startappprotection` to start App Protection component
Support for customized URLs through 301 redirects	2210		StoreFront™ to cloud store URL migration
Support for Windows 8.1 and Windows Server 2012 R2	2204.1	2204.1	Use the supported operating system as given in the System Requirements section.
Citrix Casting is installed by default	2112.1	2205	Citrix Casting can be installed on-demand with Citrix Workspace app.

ITEM	DEPRECATION ANNOUNCED IN	REMOVED IN	ALTERNATIVE
with Citrix Workspace app			**Note:** Citrix Casting is not installed by default during the Citrix Workspace app.
The **All Accounts** option in the menu for Workspace (cloud) stores only.	2112.1	2202	
The **Remember the password** option in the logon screen on Workspace app (cloud) stores.	2008	2008	
Citrix Receiver™ for Universal Windows Platform	2006	2102	
The option to add or remove descriptions for stores in the **Add or Remove accounts** dialog. The **Description** column has been deprecated.	2006.1		You can add or remove store account details without adding a description.
The option to enable or disable stores from the **Add or Remove Accounts** dialog	2006.1		
Support for Windows 7	2002	2006.1	Use the supported operating system as given in the System Requirements section. **NOTE**

ITEM	DEPRECATION ANNOUNCED IN	REMOVED IN	ALTERNATIVE
			Windows 7 is supported in Version 2002.
`/rcu` installer switch	1909		Use `/forceinstall` switch instead of `/rcu`.