Citrix Workspace app 2402 LTSR for Windows

Contents

About Citrix Workspace app 2402 LTSR for Windows

February 15, 2024

> **Important:**
>
> This documentation describes the features and configuration of Citrix Workspace app 2402 LTSR for Windows. This version is the latest Long Term Service Release (LTSR) of Citrix Workspace app for Windows.
>
> Note that this release 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 2203.1 LTSR for Windows automatically updates to Citrix Workspace app 2402 LTSR for Windows.
> - If you have enabled auto-update on your Citrix Workspace app and have opted for the CR program, Citrix Workspace app CR version automatically updates to Citrix Workspace app 2311 for Windows.
> - On Citrix Workspace app 2402 LTSR, SaaS and Web apps must be launched using the native browser on the user device. SaaS and Web apps with enhanced security controls open via Secure Browser Service within the native browser.
> - If you update from a previous CR release of Citrix Workspace app for Windows to Citrix Workspace app 2402 LTSR to Windows, the browser components (CEF and Chromium) get uninstalled. As a result, the Browser Content Redirection feature stops working, and Web and SaaS based apps are launched using the native browser instead of the Citrix Enterprise Browser (formerly Citrix Workspace Browser).

Downloads

Citrix Workspace app 2402 LTSR for Windows

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.

Baseline components

2402 LTSR baseline components	Version
XenApp and XenDesktop LTSR with CUs	7.6
XenApp and XenDesktop LTSR with CUs	7.15
Citrix Virtual Apps and Desktops 7 LTSR with CUs	1912 LTSR
Citrix Virtual Apps and Desktops 7 LTSR with CUs	2203.1 LTSR
Citrix Virtual Apps and Desktops 7 CR	2204.1 CR

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 Management Service
Citrix DaaS (formerly Citrix Virtual Apps and Desktops service)

Notable exclusions

The following features, components, and platforms are not eligible for 2402 LTSR lifecycle milestones and benefits. Specifically, cumulative updates and extended lifecycle benefits are excluded. Updates to excluded features and components will be available through regular current releases.

Excluded components and features
Browser Content Redirection
Citrix Enterprise Browser
Citrix Endpoint Analysis

Citrix Workspace app 2402 LTSR for Windows - Preview

February 22, 2024

Learn about new features and enhancements available for Citrix Workspace app 2402 LTSR for Windows.

> **Important:**
>
> Citrix Enterprise Browser, Citrix Endpoint Analysis, and Browser Content Redirection do not get Citrix Workspace app LTSR benefits (extended lifecycle and fix-only cumulative updates) as they aren't LTSR compliant. However, they're allowed to be used with Citrix Workspace app LTSR as compatible components. You must know that Citrix Workspace app LTSR includes current release updates for these components. Also, Citrix Enterprise Browser and Browser Content Redirection aren't installed by default, as they're considered optional.

What's new in 2402 LTSR

The following is a list of features that are available in Citrix Workspace app 2402 LTSR for Windows.

- 2402 LTSR

  - 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
  - Version upgrade for Chromium Embedded Framework
  - Install Microsoft teams VDI plug-in for Citrix
  - Screen Capture Allow List
  - Process exclusion list
  - USB Filter Driver Exclusion List
  - Security indicator when visiting websites
  - Citrix Enterprise Browser introduces additional settings in the Global App Configuration service

- 2311.1

  - Introducing new installer for Citrix Workspace app
  - Support for Activity Manager in cloud stores
  - Automatic selection of video codec
  - Loss tolerant mode for audio
  - Synchronize multiple keyboards at session start
  - Improved performance of BCR
  - Version upgrade for Chromium Embedded Framework
  - Important update on App Protection file and driver names
  - Enhancement to background blurring and effects for Microsoft Teams optimization with HDX
  - Citrix Enterprise Browser

- 2309.1

  - Citrix Enterprise Browser

- 2309

  - Additional .NET prerequisites
  - Improved virtual apps and desktops launch experience
  - Addition of the Troubleshooting option in the system tray of Citrix Workspace app
  - Sustainability initiative from Citrix Workspace app
  - Commands to configure keyboard layout synchronization using command-line interface
  - Command to cleanup and install Citrix Workspace app
  - Optimized Microsoft Teams updates
  - App Protection
  - Authentication through Citrix Enterprise Browser

- 2307

  - Added support for playing short tones in optimized Microsoft Teams
  - Citrix Enterprise Browser

- 2305.1

  - Improved virtual apps and desktops launch experience
  - Tracking Storebrowse command status
  - Support for modern authentication methods for StoreFront stores
  - Support for more than 200 groups in Azure AD
  - App Protection
  - Citrix Enterprise Browser

- 2303

  - Configure path for Browser Content Redirection overlay Browser temp data storage
  - Support for modern authentication methods for StoreFront stores
  - Improved experience for optimized Microsoft Teams video conference calls
  - Enhancement to App Protection: Anti-DLL Injection
  - Citrix Enterprise Browser
  - Secure Private Access support for StoreFront

- 2302

  - Improved virtual apps and desktops reconnection experience
  - Client App Management for Zoom plug-in
  - Updated audio device selection behavior for optimized Microsoft Teams
  - App Protection enhancement
  - Citrix Enterprise Browser

- 2212

  - Client App Management
  - Auto-update version control
  - Force login prompt for Federated identity provider
  - Improved reconnection experience after connection lease file expiry
  - Support for default installation of App Protection
  - App Protection enhancement: Screen capture detection and notification
  - Desktop Viewer optimization
  - Citrix Enterprise Browser

- 2210.5

  - Enhancement to auto-update
  - Citrix Enterprise Browser

- 2210
  - Background blurring for webcam redirection
  - App Protection enhancements for web and SaaS apps on Windows 11
  - Limiting video resolutions
  - Rebranding Citrix Workspace Browser
  - Open all web and SaaS apps through the Citrix Enterprise Browser
  - Supporting auto-update of Citrix Workspace app on VDA
  - Citrix Enterprise Browser (formerly Citrix Workspace Browser)
- 2207
  - Background blurring and effects for Microsoft Teams optimization with HDX
  - Improved auto-update experience
  - Note on Citrix Workspace app update
- 2206
  - Improved graphics performance
  - Enabling DPI matching
  - Citrix Enterprise Browser
- 2205
  - Change to Citrix Casting
  - Quick access to resources
  - Sign out custom web store upon Citrix Workspace app exit
  - Support to open Citrix Workspace app in maximized mode
  - Storebrowse support for Workspace
  - Citrix Enterprise Browser
- 2204.1
  - Audio redirection enhancement
  - Citrix Enterprise Browser
  - Microsoft Teams optimization

2402 LTSR features

Sustainability initiative for cloud hybrid launch

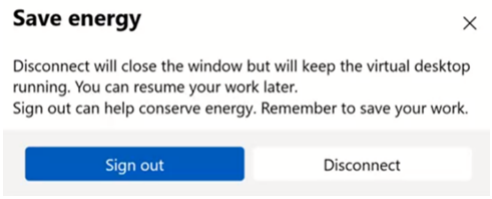
> **Note:**

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

From Citrix Workspace app 2402 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.

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:



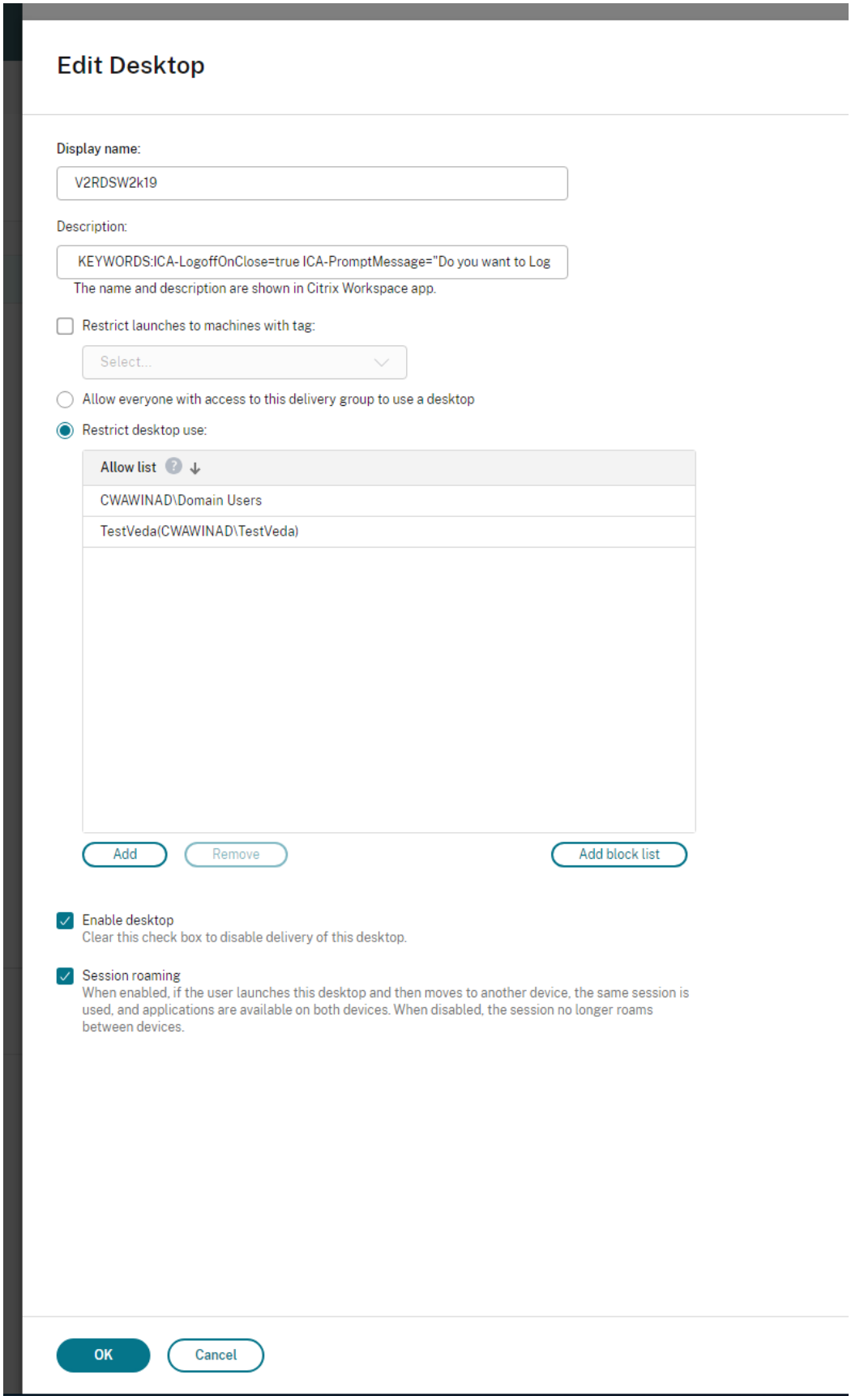
Customize the text in the Saved energy screen You can also customize the text that appears on the **Save energy** screen.

1. Follow steps 1–8 in the preceding section.
2. Set the `ICA-PromptMessage` keyword to the required text in the **Description** field.

   > **Note:**
   >
   > The maximum number of characters allowed in the Description field is 200.

   Example:

```
KEYWORDS:ICA-LogOffOnClose=true ICA-PromptMessage="Do you want to
    Log off?"
<!--NeedCopy-->
```

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
<!--NeedCopy-->
```

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.

3. Click **OK**. The following dialog box appears when you close the virtual desktop.

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.

This approach of 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.

> **Note:**
>
> This feature isn't supported on 32-bit Windows 10 and on Windows Server 2016.

System requirements:

- Citrix Workspace app 2309 or later
- Citrix Virtual Apps and Desktops 2308 or later

Supported VDA OS versions:

- For multi-session:
  - Windows Server 2019
  - Windows Server 2022
- For single-session:
  - Windows 10 version 22H2
  - Windows 11 version 22H2

Prerequisites:

- The client or endpoint must be connected to the domain.
- Requires a direct line of sight of Active Directory.

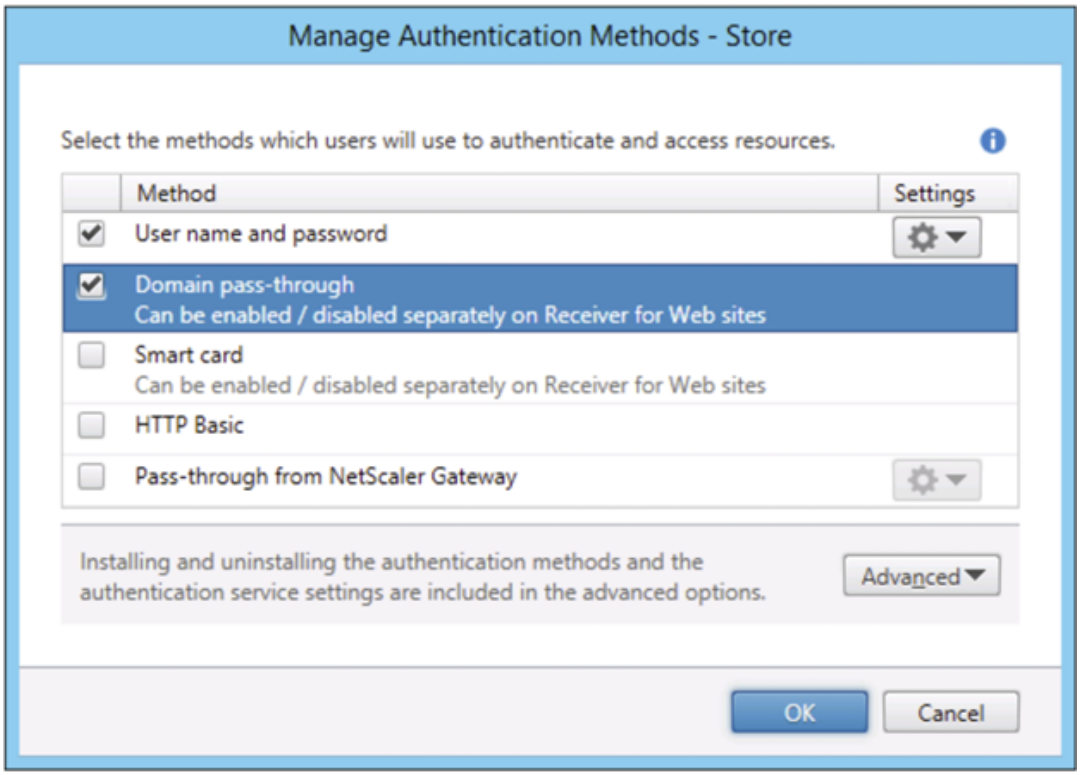
StoreFront and DDC settings Setup a domain pass-through environment using the following settings:

> **Note:**
>
> You can skip this step if you have already configured the domain pass-through in your environment.

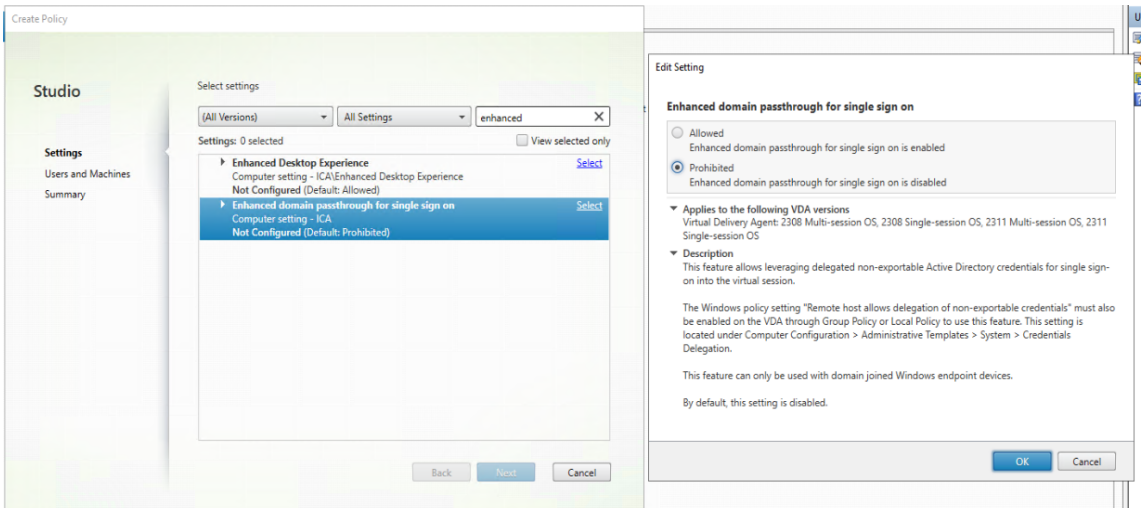
1. When Citrix Workspace app is configured on the StoreFront:
   a) Open **StoreFront Studio**.
   b) Go to **Store** > **Manage Authentication methods**.
   c) Enable **Domain pass-through**.

Or,

1. When using Citrix Workspace app through the browser:
   a) Open StoreFront.
   b) Open **Stores** > **Receiver for Websites** > **Manage Authentication** methods.
   c) Enable **Domain pass-through**.



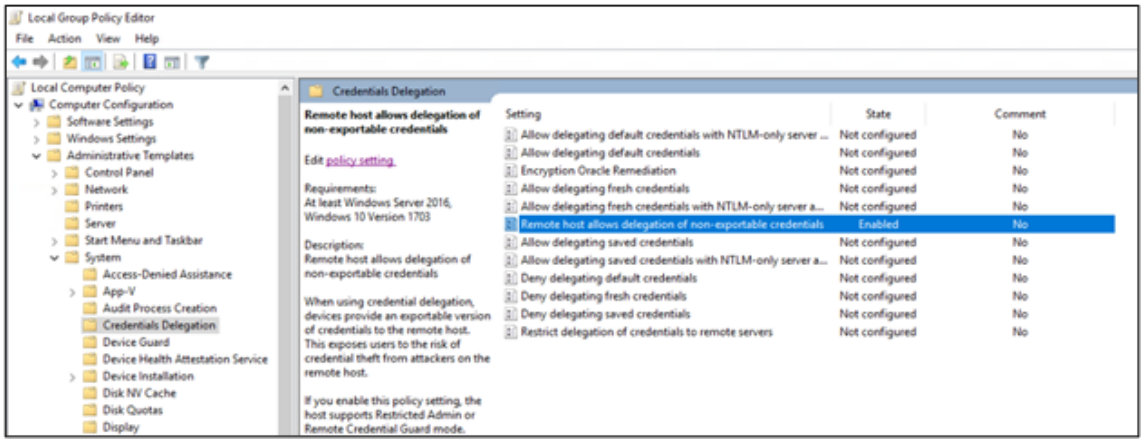
2. Enable **Enhanced domain passthrough for single sign on** policy on DDC.



3. Click **OK**.

VDA settings

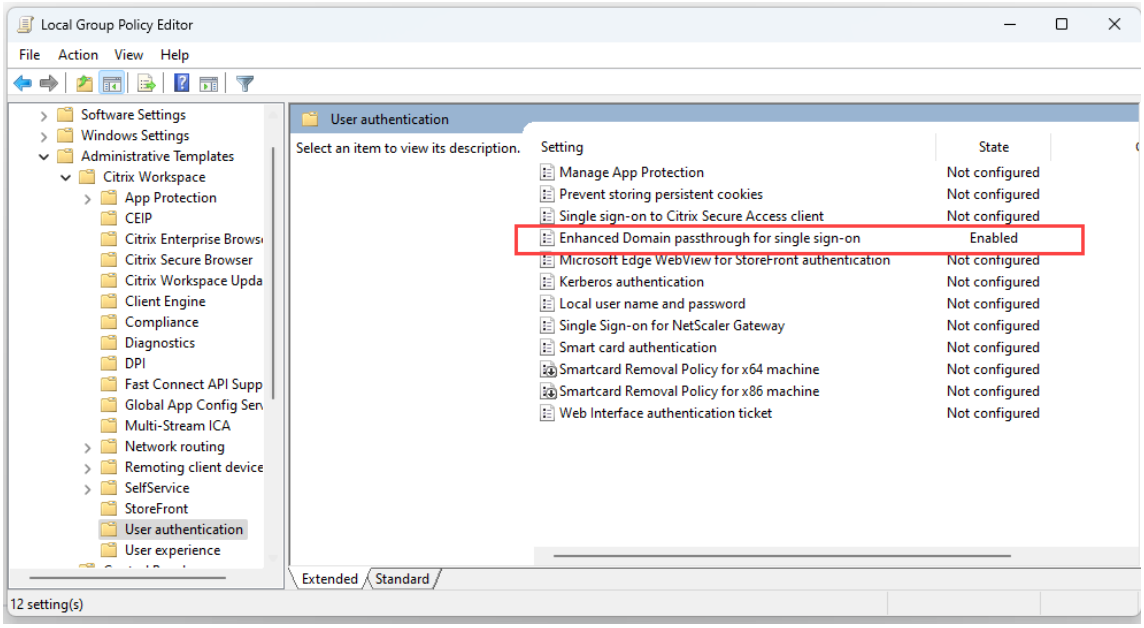
1. Navigate to **Computer Configuration\Administrative Templates\System\Credentials Delegation** on VDA.
2. Enable **Remote host allows delegation of non-exportable credentials** windows policy on VDA.

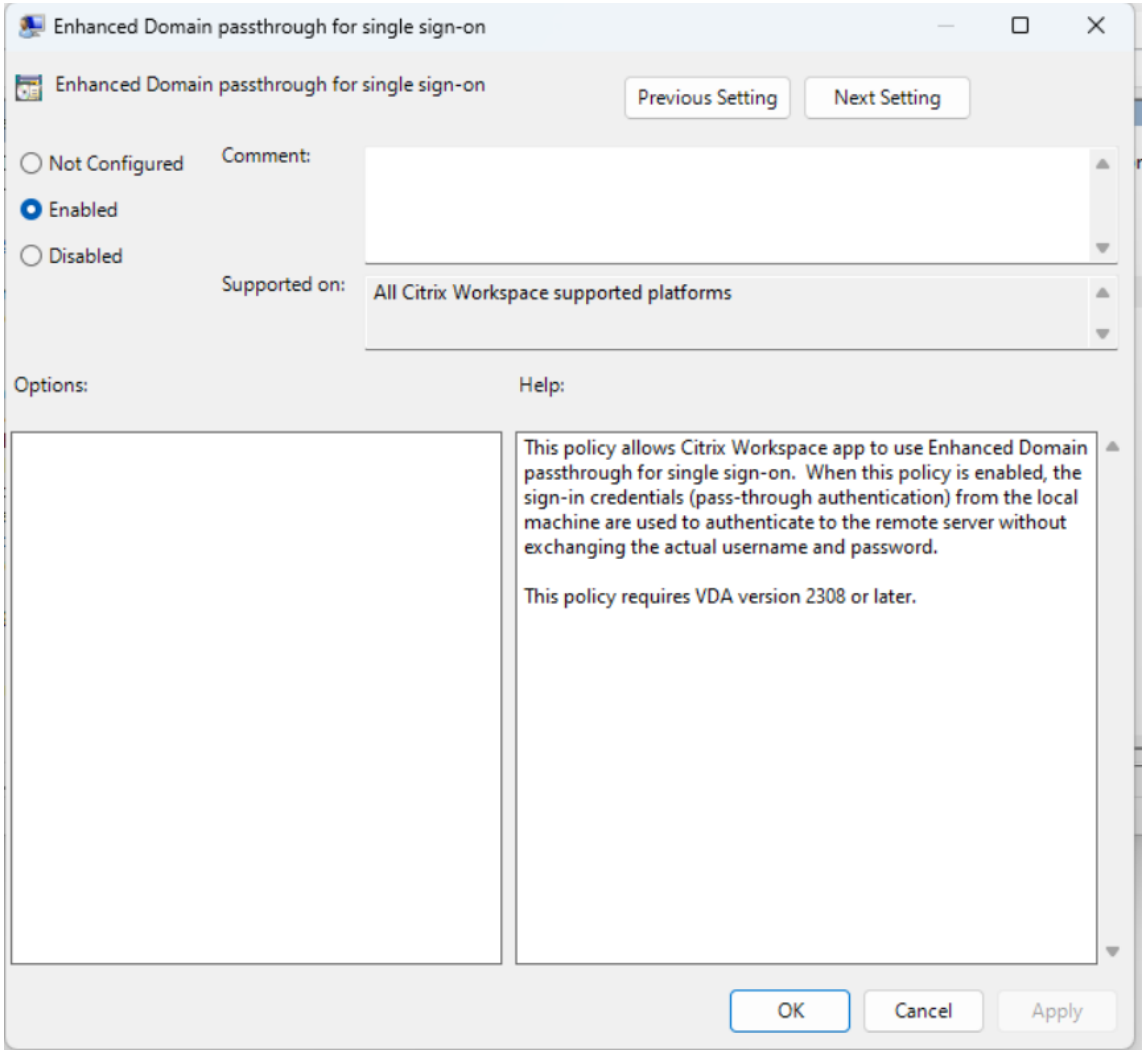


3. Reboot the VDA machine.

Client settings

1. Ensure that the client machine is domain joined.
2. Ensue that the client machine is 64-bit.
3. Open **Group Policy Editor**.
4. Navigate to **Computer Configuration\Administrative Templates\Citrix Components\Citrix Workspace\User Authentication**.
5. Configure the **Enhanced Domain passthrough for single sign-on** group policy.





6. Modify the **Internet Options** settings on the client.

> **Note:**
>
> You can skip this step if you have already configured the domain pass-through in your environment.

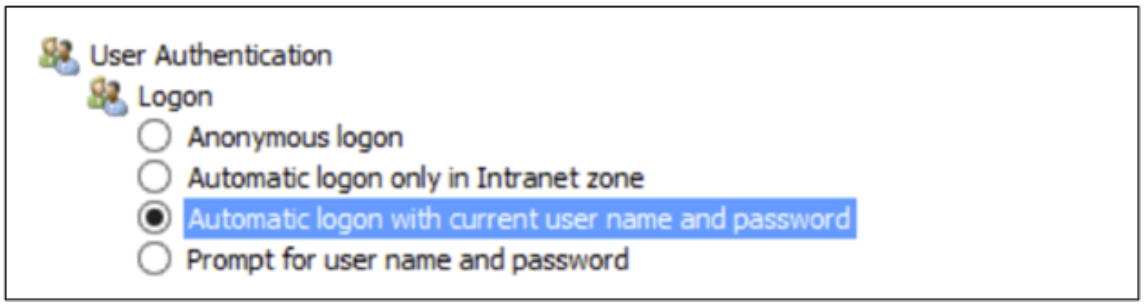
1. Add the StoreFront server to the list of trusted sites using **Internet Options**. To add:

    a) Open **Internet Options** from the **Control Panel** > **Network and Internet**.
    b) Click **Security** > **Local Intranet** and click **Sites**. The **Local Intranet** window appears.
    c) Click the **Advanced** tab.
    d) Add the URL of the StoreFront FQDN with the appropriate HTTP or HTTPS protocols.
    e) Click **Close** and **OK**.

2. Modify the User Authentication settings in Internet Explorer. To modify:

    a) Open **Internet Options** from the **Control Panel** > **Network and Internet**.

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**.



3. Click **OK**.

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.

Version upgrade for Chromium Embedded Framework

The version of the Chromium Embedded Framework (CEF) is upgraded to 120. This version upgrade helps to resolve security vulnerabilities.

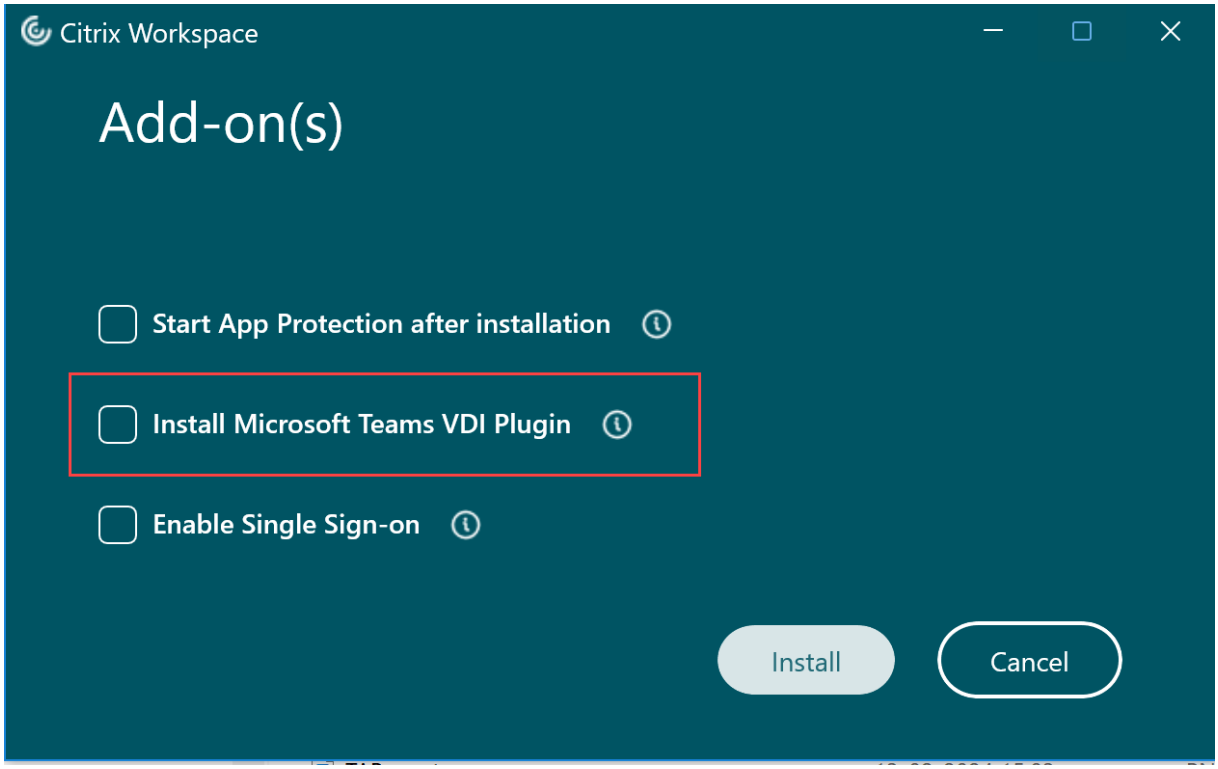
Install Microsoft Teams VDI plug-in for Citrix

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

> **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`

If installation is being done via `ADDLOCAL` parameter, then use `mtopbootstrapperinstaller` as parameter value.
For example: CitriWorksapceApp.exe ADDLOCAL=mtopbootstrapperinstaller
Description

App Protection

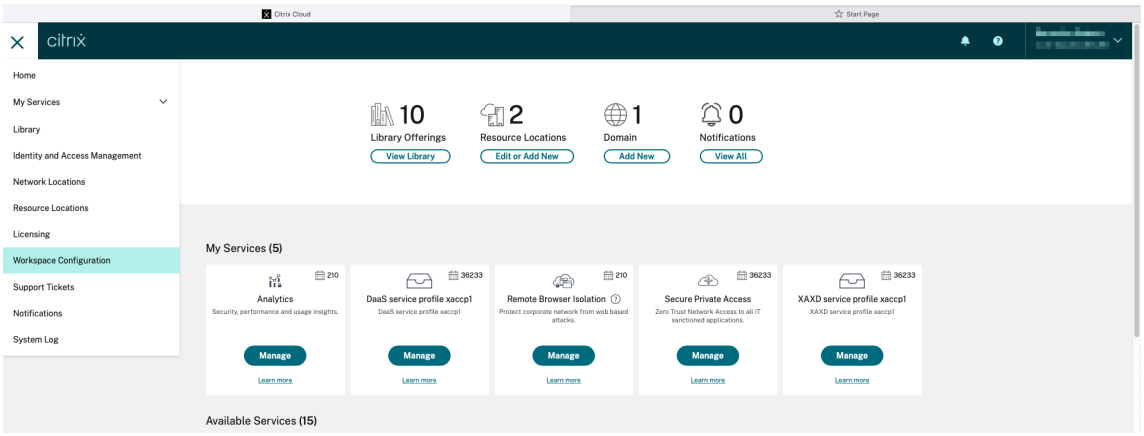
Screen Capture Allow List If Citrix Workspace app, virtual apps and desktops, or SaaS apps are enabled with the App Protection Anti-screen capture policy, then you can't capture their screens using any screen-capturing tool.

However, starting from the Citrix Workspace app for Windows 2402 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. To add an app to the screen capture allow list, see Configure the Screen Capture Allow List.

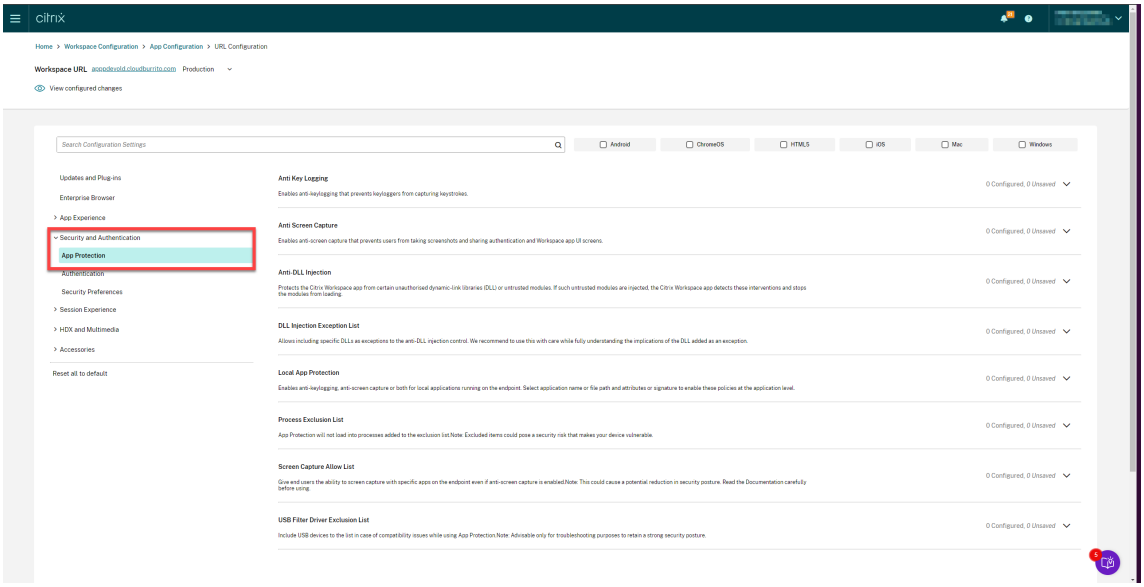
> **Important:**
>
> It isn't recommended to run an allow-listed app on your device for a longer period because it decreases the security posture. You can use the allow-listed apps for sharing your screen temporarily during scenarios such as troubleshooting. It is recommended to adhere to the following conditions:
>
> - Run the allow-listed app for a short period along with the resource enabled with the App Protection Anti-screen capture feature.
> - Terminate the allow-listed app immediately after the required task is completed.
> - Add a watermark when sharing the screen while using the resource enabled with the App Protection Anti-screen capture feature for more security.

Configure the Screen Capture Allow List To add an app to the screen capture allow list, do the following steps:

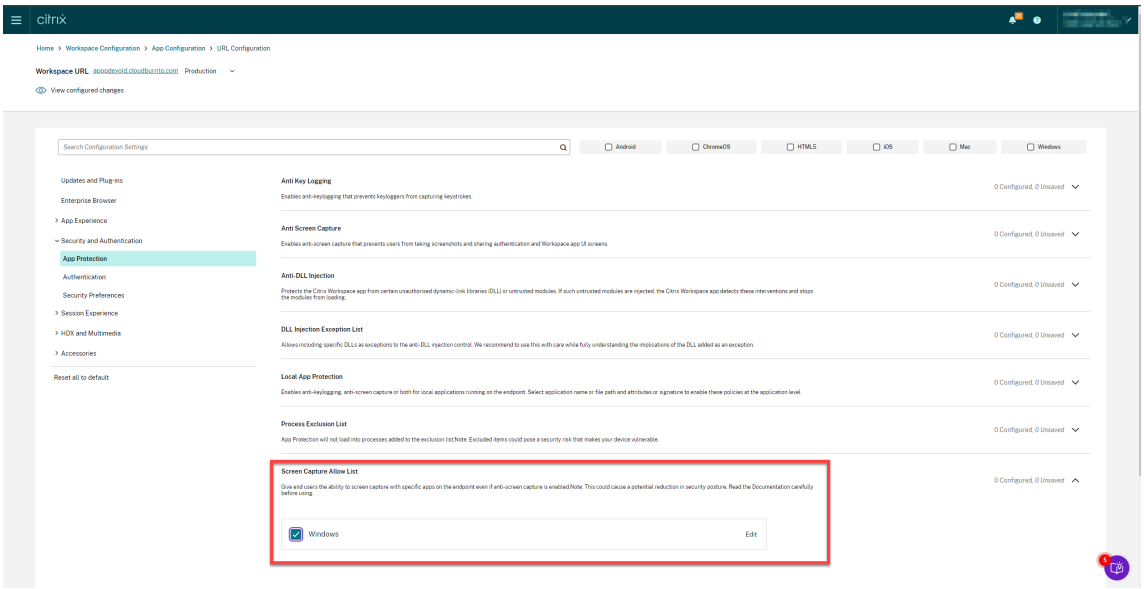
1. Sign in to your Citrix Cloud account and select **Workspace Configuration**.



2. Select **App Configuration** > **Security and Authentication** > **Configure** > **App Protection**.



3. Click **Screen Capture Allow List** and select the **Windows** checkbox.



4. Click the **Edit** option.

   The **Manage settings for Windows** screen appears.

5. Add the information about the app that you want to add to the Screen Capture Allow List.

   For example,

```
[
 {

 "name": "ScreenshotTool_1.exe",
 "signature": "ScreenshotTool_1 Signature",
 "publisher": "ScreenshotTool_1 Publisher"
```



```
  }
 ,
 {

  "name": "Screenshottool_2.exe",
  "signature": "",
  "publisher": ""
  }

]
<!--NeedCopy-->
```

Manage settings for Windows

```
[
  {
    "name": "ScreenshotTool_1.exe",
    "signature": "ScreenshotTool_1_Signature",
    "publisher": "ScreenshotTool_1_Publisher"
  },
  {
    "name": "ScreenshotTool_2.exe",
    "signature": "",
    "publisher": ""
  }
]
```

Save draft Cancel

Note:

- The `name` has to be mandatorily filled. At the same time, the `publisher` and `signature` aren't mandatory. However, It's recommended to add the relevant`publisher` and `signature` to ensure that only the allow listed app can take the screenshots.

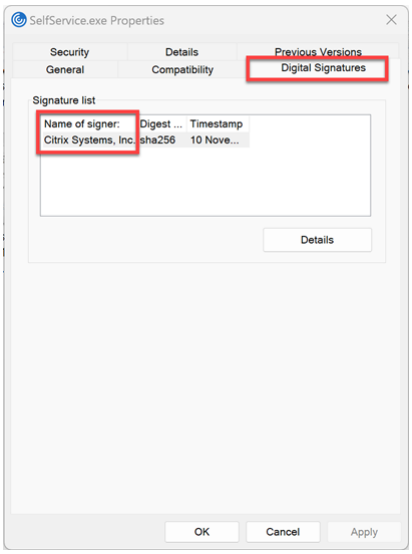
> - Without `publisher` and `signature` values, a malicious application with the same name can capture screenshots.
> - Also, you can add multiple apps to the Screen Capture Allow-list by adding multiple entries in this block.

To get the `publisher` and `signature` information, do the following steps:

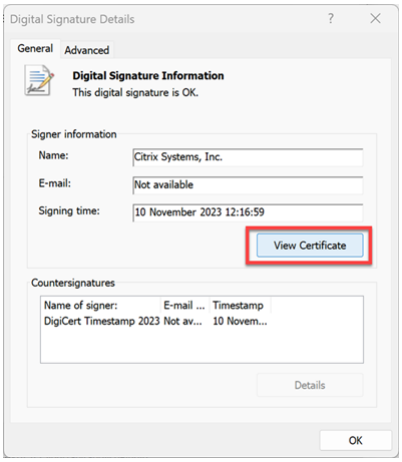
a) Open the file location where you have the relevant `.exe` file of the app.

b) Right-click on the `.exe` file and then click **Properties**. A properties pop-up screen appears.

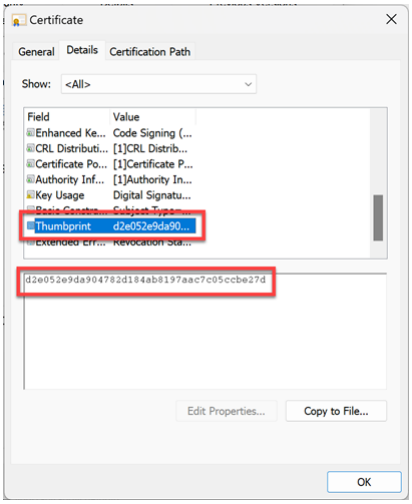
c) Click **Digital Signatures**. The **Name of signer** is the `publisher` value.



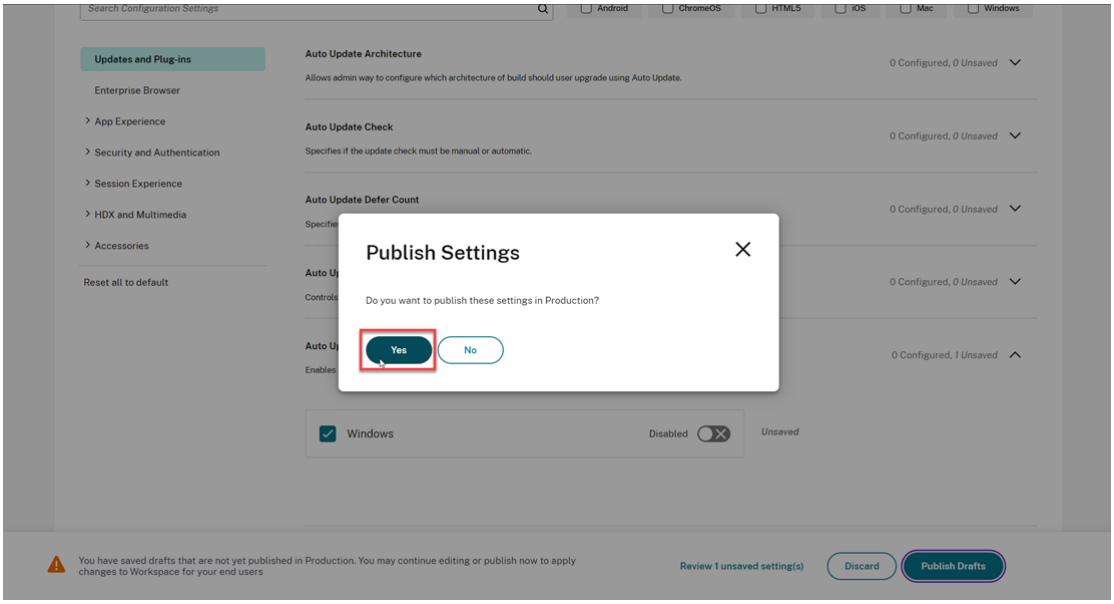
d) Click the first entry in the **Name of signer** and then click **Details** > **View Certificate**.



e) Click **Details** > **Thumbprint**. The content that appears in the textbox is the `signature`.



6. Click **Save draft** and then click **Publish Drafts**.
7. On the **Publish Settings** dialog box, click **Yes**.



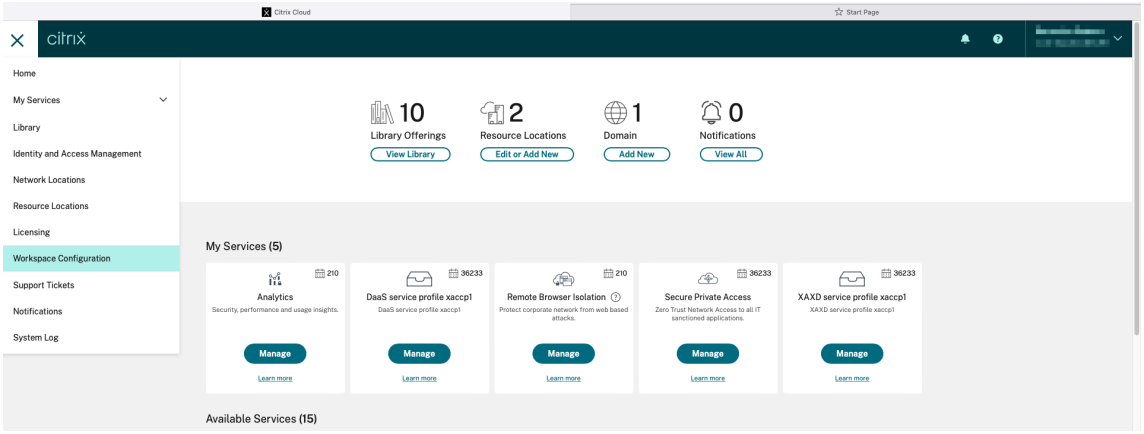
Process exclusion list When you launch any process or application on your device, App Protection DLLs are injected into each process if the App Protection is enabled. Sometimes, this might cause the process or application not to work due to compatibility issues with the DLL.

Starting from the Citrix Workspace app for Windows 2402 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. To configure the Process exclusion list, see Configure Process exclusion list.

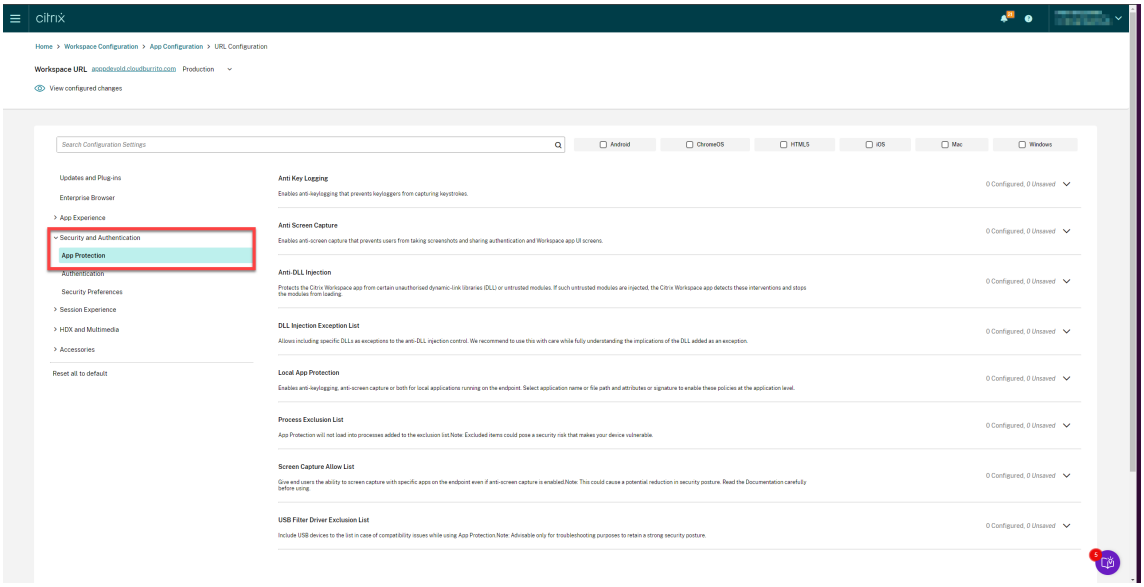
> **Important:**
>
> It's not recommended to exclude processes as it decreases the security posture. You can use this to temporarily unblock the usage of the application and raise a support ticket for further investigation.

Configure Process exclusion list To add a process to the Process Exclusion List, do the following steps:

1. Sign in to your Citrix Cloud account and select **Workspace Configuration**.



2. Select **App Configuration** > **Security and Authentication** > **Configure** > **App Protection**.



3. Click **Process Exclusion List** and then select the **Windows** checkbox.
4. Click the **Edit** option.

   The **Manage settings for Windows** screen appears.

5. Add the information about the process that you want to add to the Process Exclusion List.

   For example,

```
[
 {

  "name": "sample_program.exe",
  "publisher": "sample_publisher1",
  "signature": "sample_thumbprint1"
  }

]
<!--NeedCopy-->
```

Manage settings for Windows

Save draft Cancel

Note:

- The `name` has to be mandatorily filled. At the same time, the `publisher` and `signature` aren't mandatory. However, It's recommended to add `publisher`

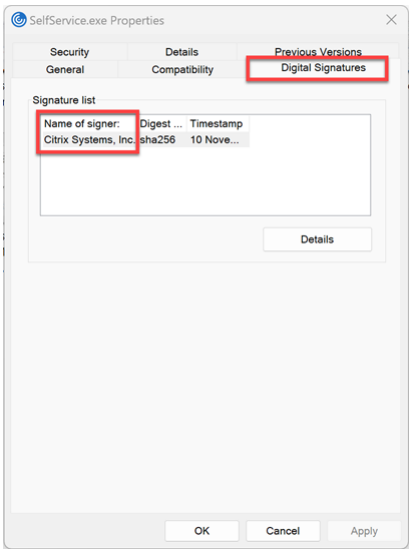
> and `signature` to ensure that the correct process is added to the list.
> - Also, you can add multiple processes to the Process Exclusion List by adding multiple entries in this block.

To get the `publisher` and `signature` information, do the following steps:

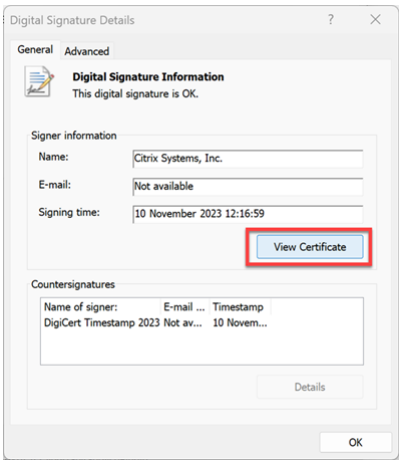
a) Open the file location where you have the relevant `.exe` file of the app.

b) Right-click on the `.exe` file and then click **Properties**. A properties pop-up screen appears.

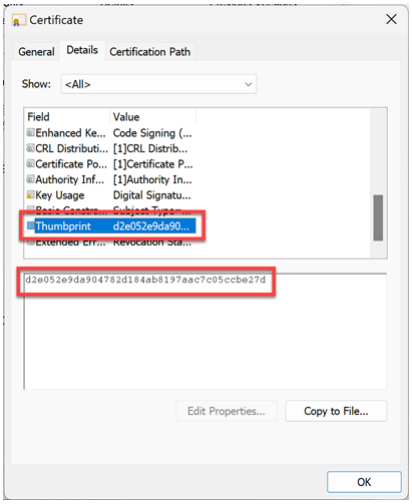
c) Click **Digital Signatures**. The **Name of signer** is the `publisher` value.



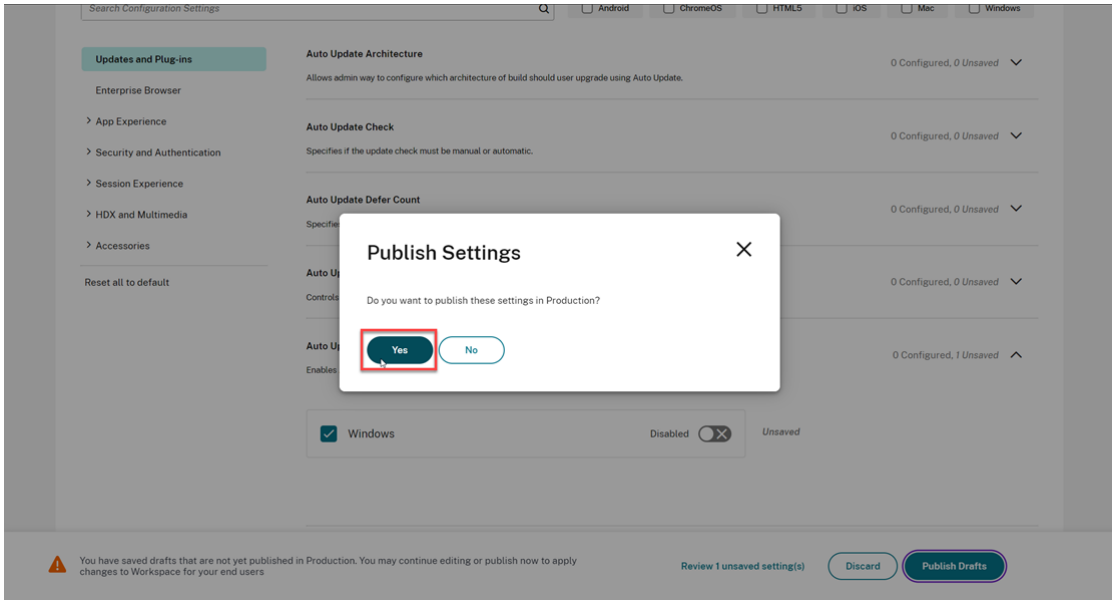
d) Click the first entry in the **Name of signer** and then click **Details** > **View Certificate**.



e) Click **Details** > **Thumbprint**. The content that appears in the textbox is the `signature`.



6. Click **Save draft** and then click **Publish Drafts**.
7. On the **Publish Settings** dialog box, click **Yes**.



8. Restart Citrix Workspace app.

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 2402 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. To add any device to the USB Filter Driver Exclusion List, see Configure USB Filter Driver Exclusion List.

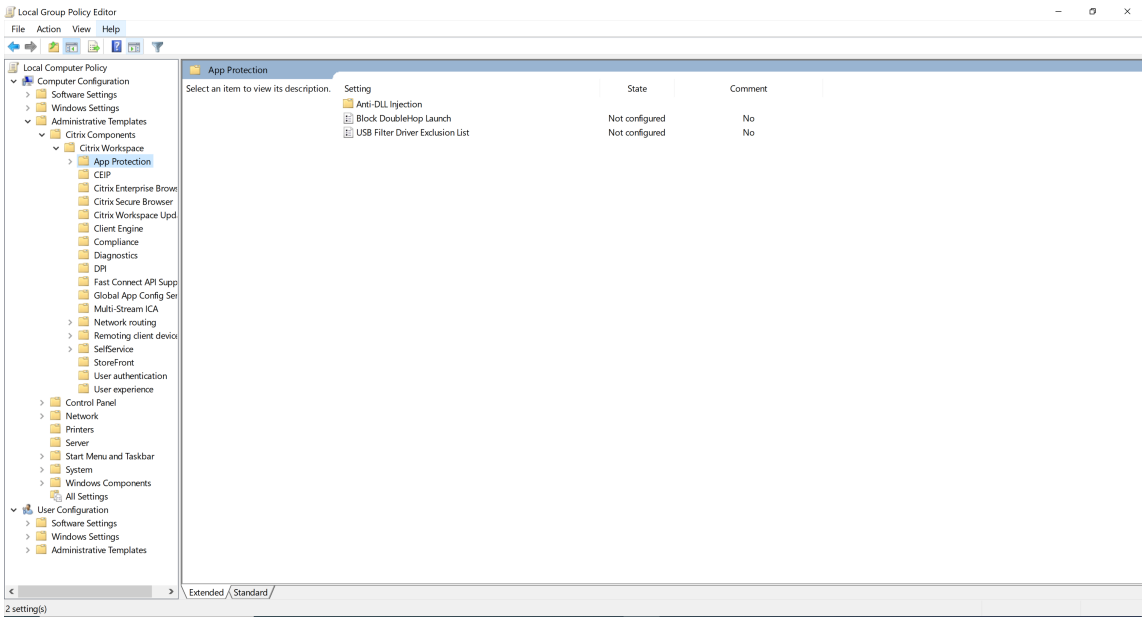
> **Note:**
>
> It isn't recommended to exclude devices permanently. Use this feature to temporarily unblock the user from using the device and raise a support ticket to investigate the compatibility issue further.

Configure USB Filter Driver Exclusion List You can add a USB device to the USB Filter Driver Exclusion List using one of the following methods:

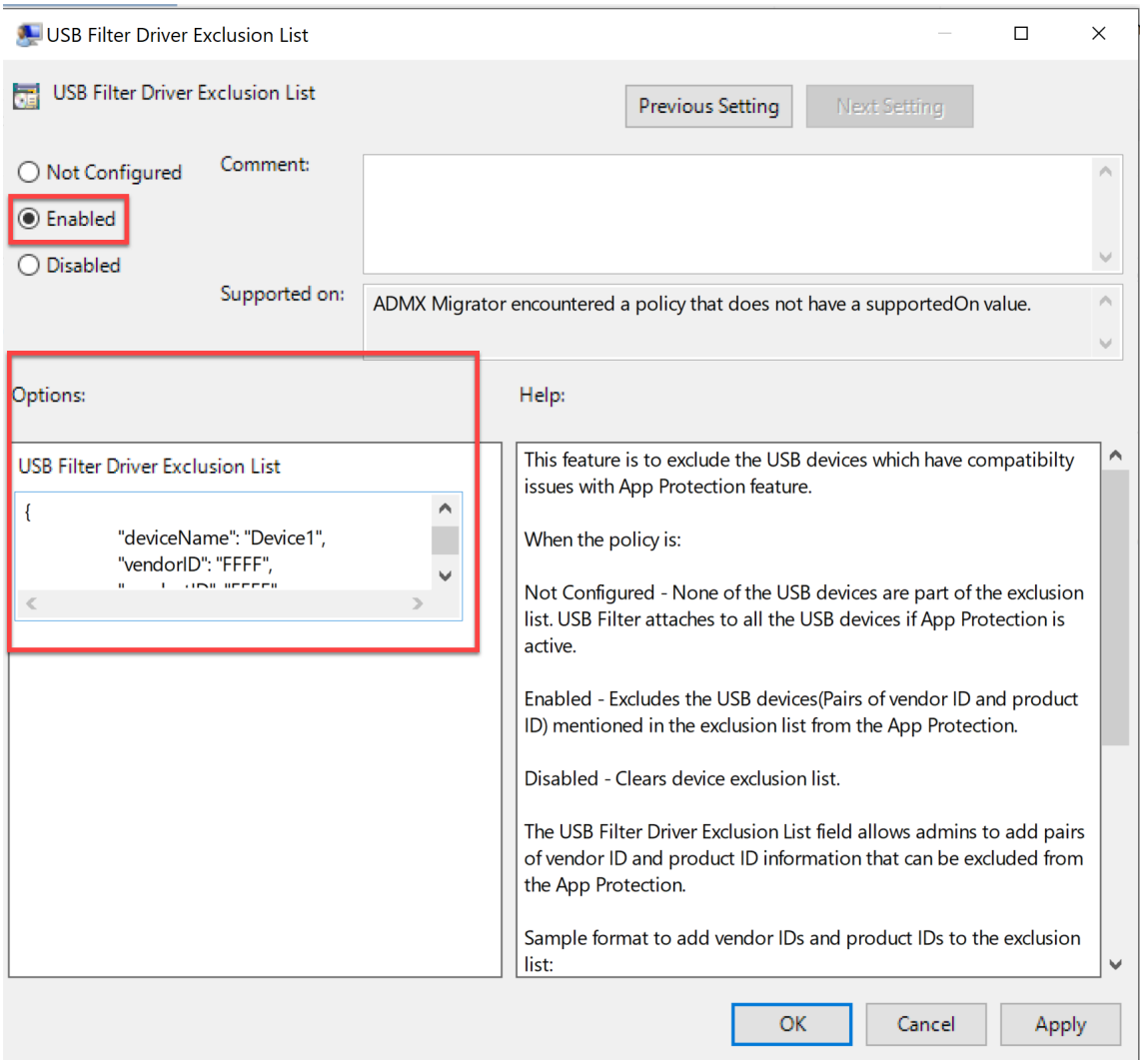
- Using Group Policy Object
- Using the Global App Configuration Service UI

Using Group Policy Object

1. Open the Citrix Workspace app Group Policy Object administrative template by running `gpedit.msc`. For more information, see Group Policy Object.
2. Under the **Computer Configuration** node, go to **Administrative Templates** > **Citrix Components** > **Citrix Workspace** > **App Protection** > **USB Filter Driver Exclusion List**.



3. Select **Enabled** and enter the **Vendor ID** and **Product ID** of the USB device you want to exclude in the **Options** text box.



> **Note:**
>
> - The `productID` and `vendorID` must be mandatorily filled. At the same time, the `deviceName` isn't mandatory.
> - Also, you can add multiple USB devices to the exclusion list by adding multiple entries in this block.

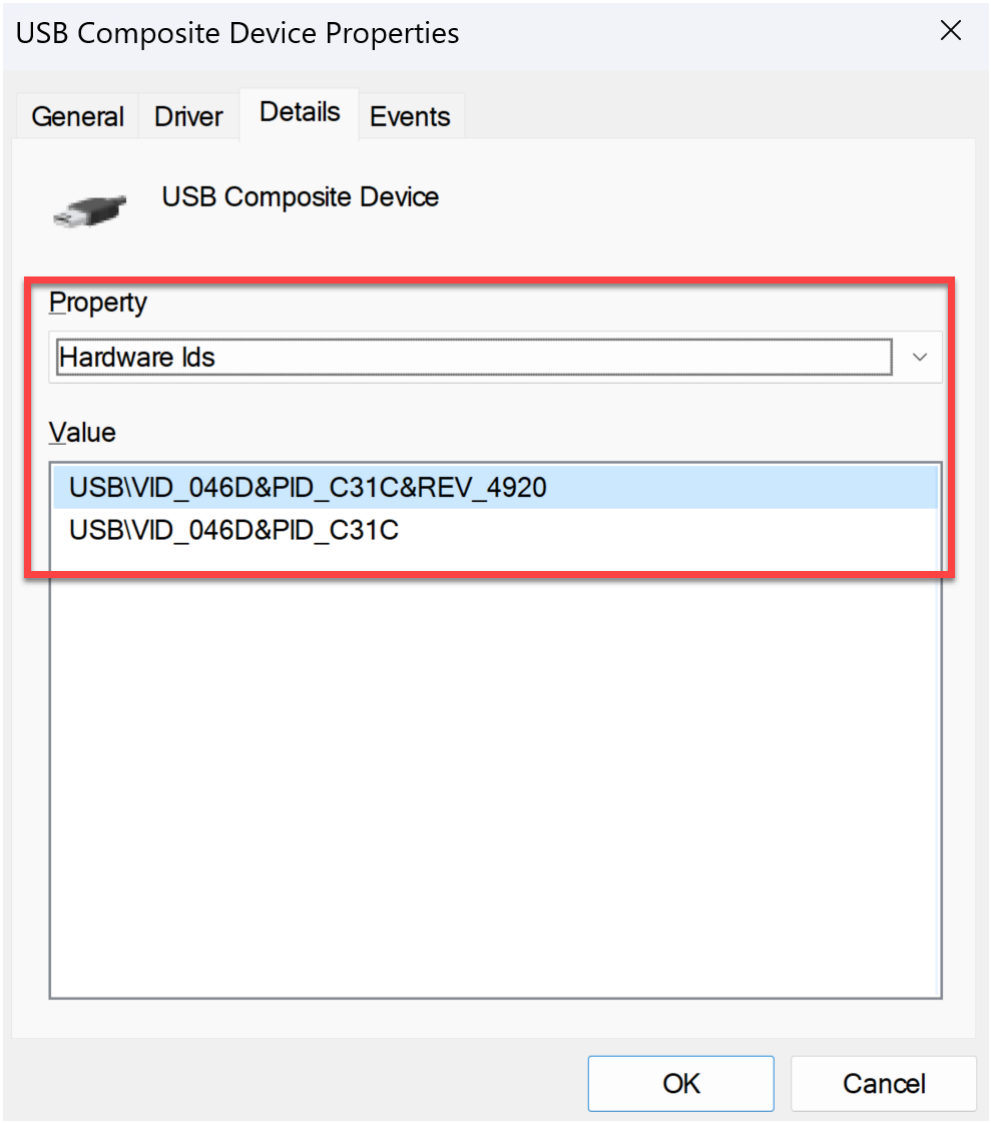
To get the `productID` and `vendorID`, do the following steps:

a) Open **Device Manager** and find the device that you want to add to the exclusion list.

b) Right-click on the device name and then click **Properties**. A properties pop-up screen appears.

c) Click **Details** and then select the **Hardware Ids** option from the **Property** list.

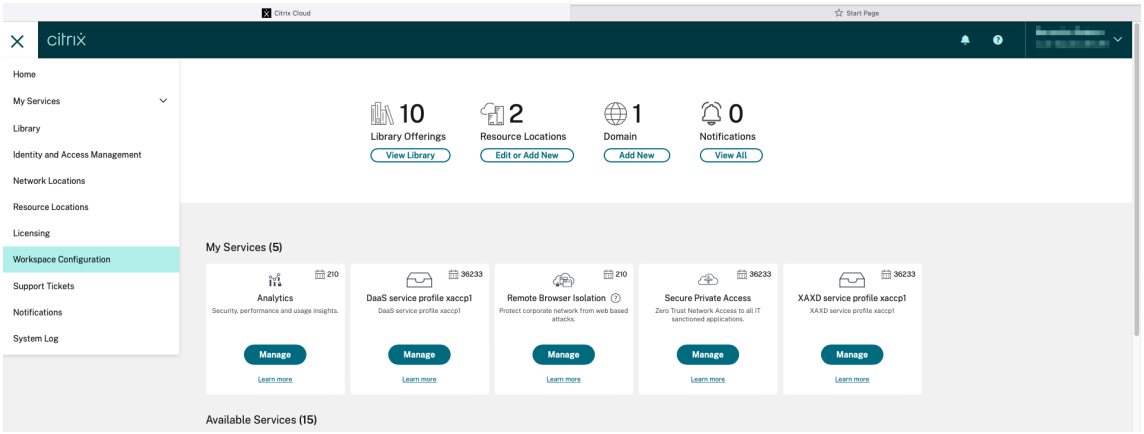
d) In the **Value** field, the value with prefix of `VID_` is the `vendorID` and the value with prefix of `PID_` is the `productID`.



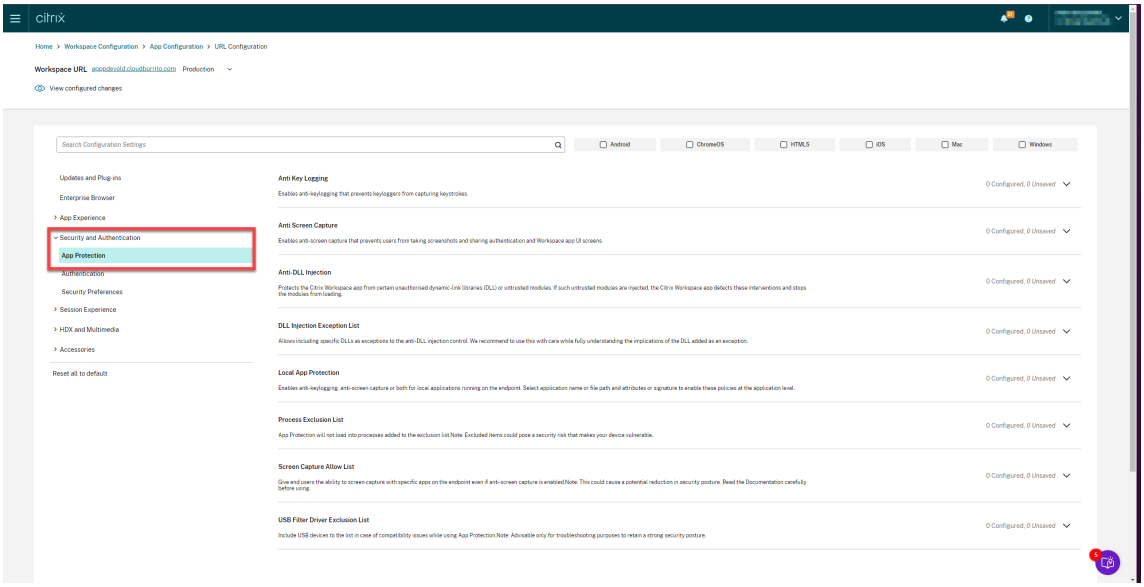
4. Click **OK**.

Using the Global App Configuration Service UI

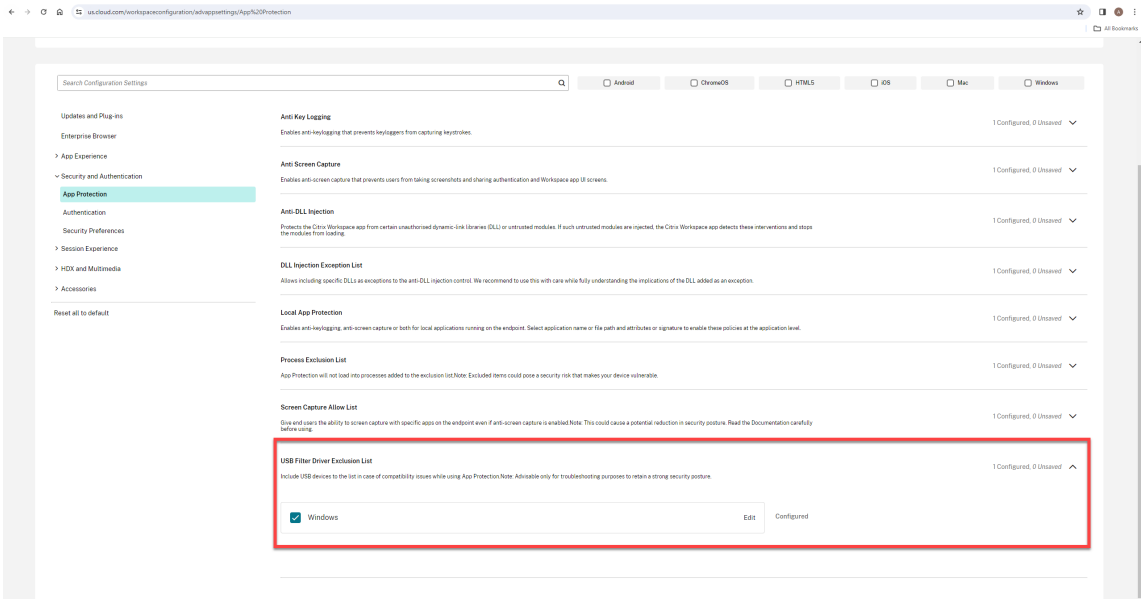
1. Sign in to your Citrix Cloud account and select **Workspace Configuration**.



2. Select **App Configuration** > **Security and Authentication** > **Configure** > **App Protection**.



3. Click **USB Filter Driver Exclusion List** and then select the **Windows** checkbox.



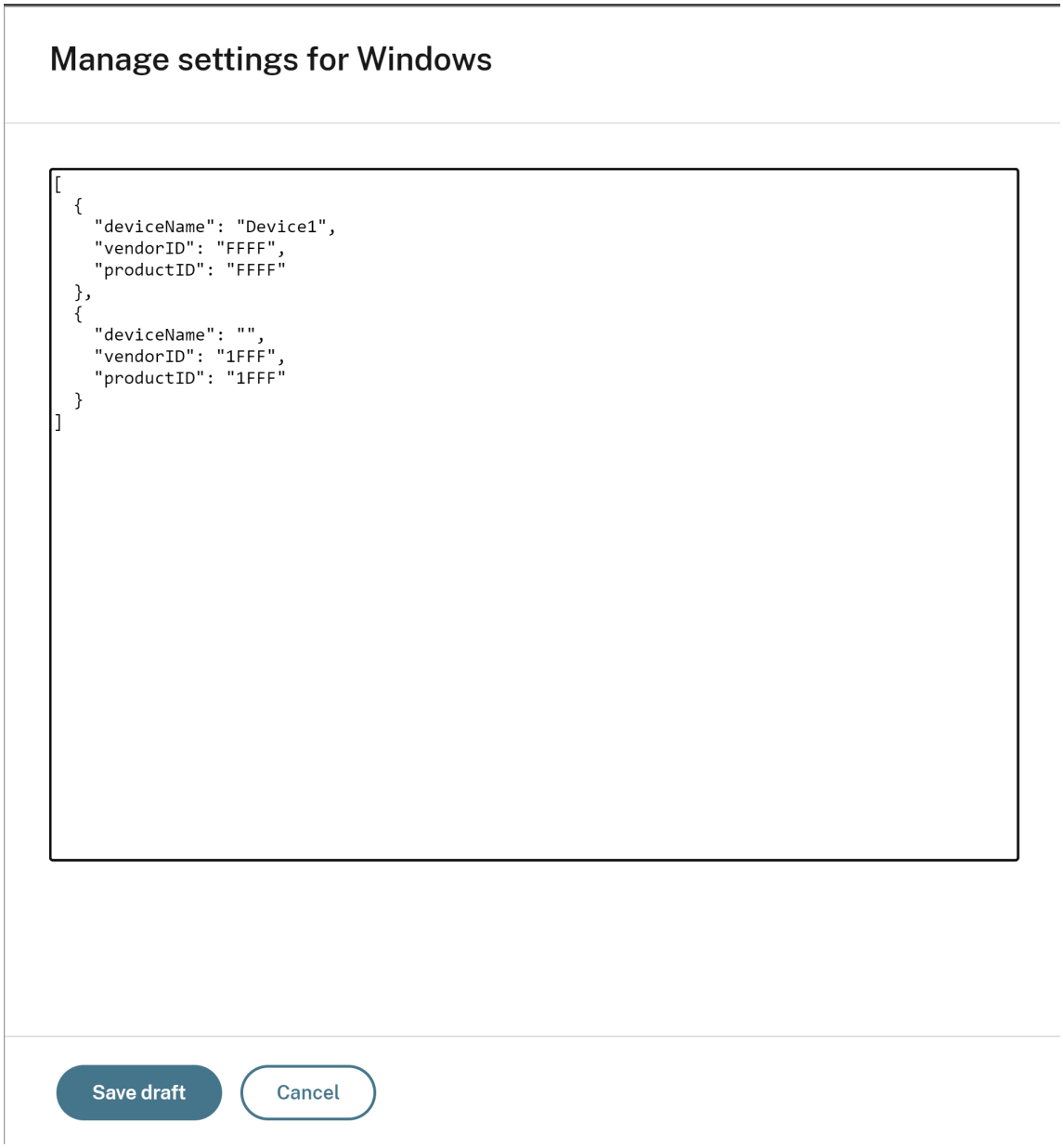
4. Click the **Edit** option.

   The **Manage settings for Windows** screen appears.

5. Add the information about the process or app that you want to add to the USB Filter Driver Exclusion List.

   For example,

```
[
 {

  "deviceName": "Device1",
  "vendorID": "FFFF",
  "productID": "FFFF"
  }

]
<!--NeedCopy-->
```

Note:

- The `productID` and `vendorID` must be mandatorily filled. At the same time, the `deviceName` isn't mandatory.
- Also, you can add multiple USB devices to the exclusion list by adding multiple entries in this block.

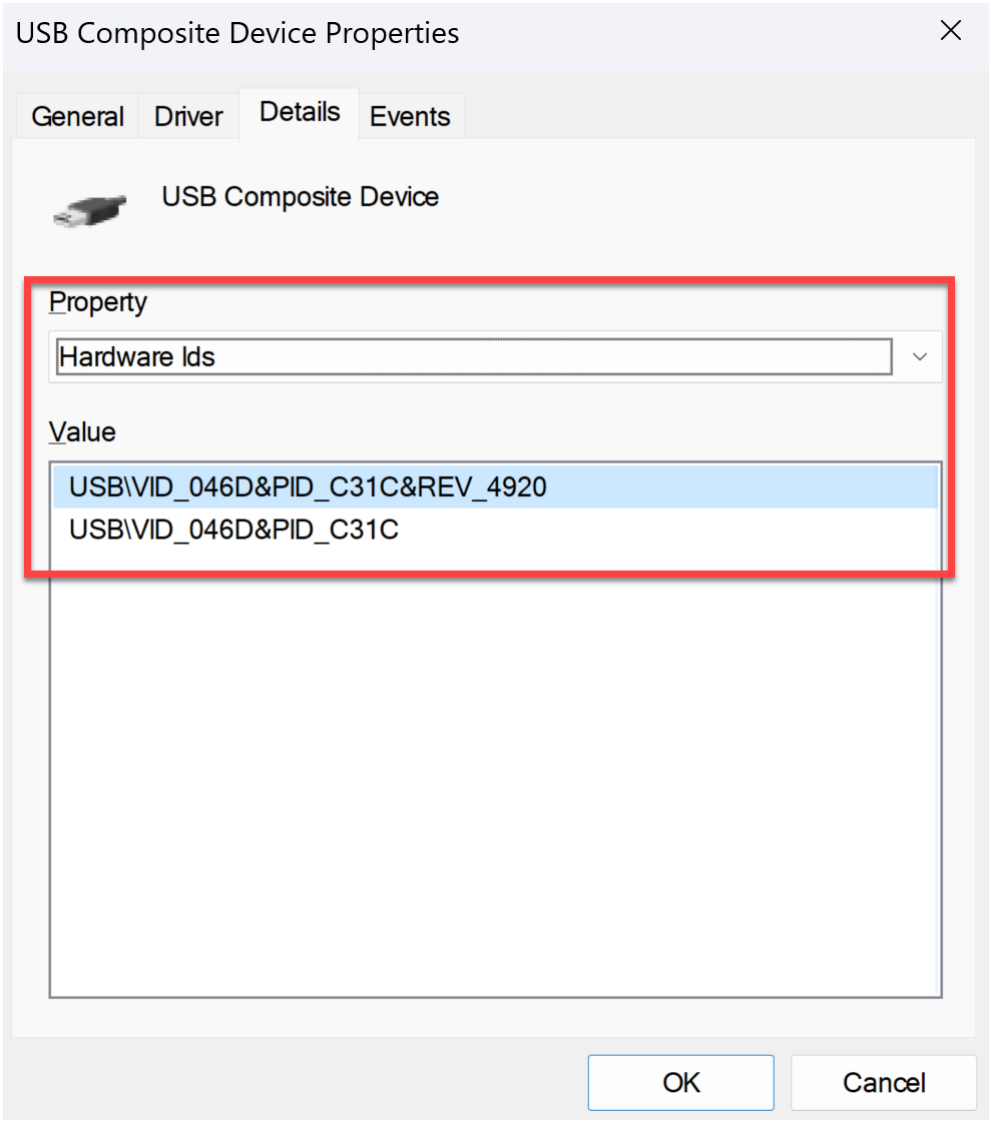
To get the `productID` and `vendorID`, do the following steps:

a) Open **Device Manager** and find the device that you want to add to the exclusion list.

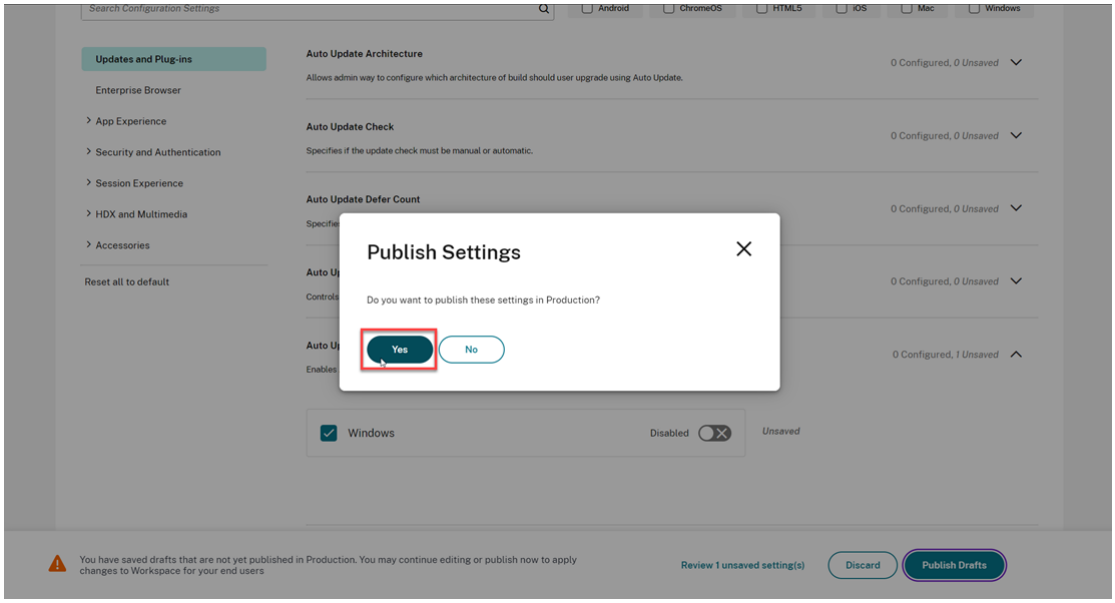
b) Right-click on the device name and then click **Properties**. A properties pop-up screen appears.

c) Click **Details** and then select the **Hardware Ids** option from the **Property** list.

d) In the **Value** field, the value with prefix of `VID_` is the `vendorID` and the value with prefix of `PID_` is the `productID`.



6. Click **Save draft** and then click **Publish Drafts**.
7. On the **Publish Settings** dialog box, click **Yes**.

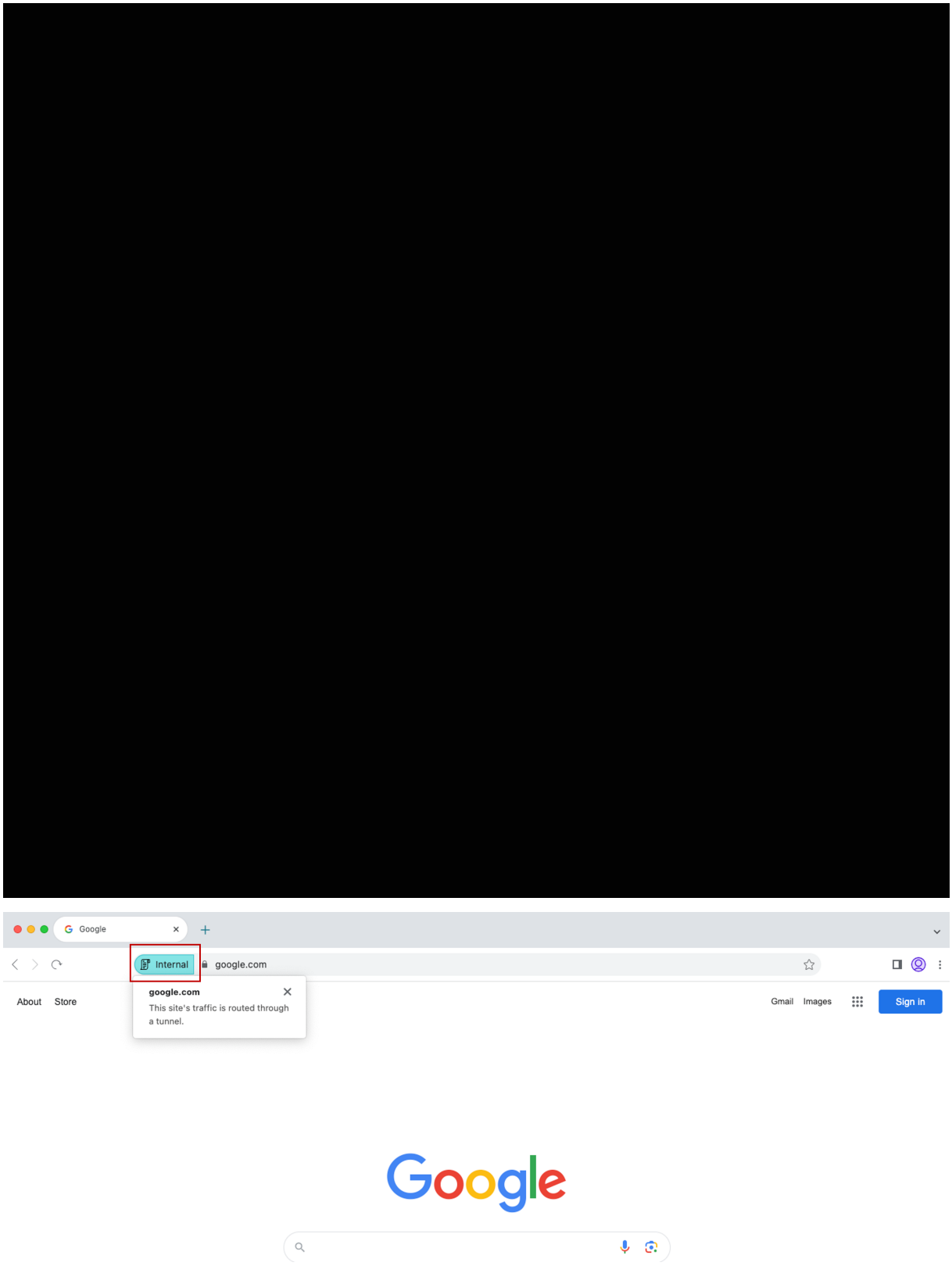


8. Restart Citrix Workspace app.

Citrix Enterprise Browser

This release of Citrix Enterprise Browser is installed with Citrix Workspace app for Windows 2402, and it's based on the Chromium version 121.

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 additional settings in the Global App Configuration service
Additional 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.

Enable autofill address When you enable the autofill address setting, Autofill suggests or fills in address information.

Configuration through API

To configure, here's an example JSON file to enable autofill address. Setting the value to 'true' autofills the address, whereas 'false' disables it.

```
"settings": [{

      "name": "auto fill address enabled",
      "value": true
   }
```

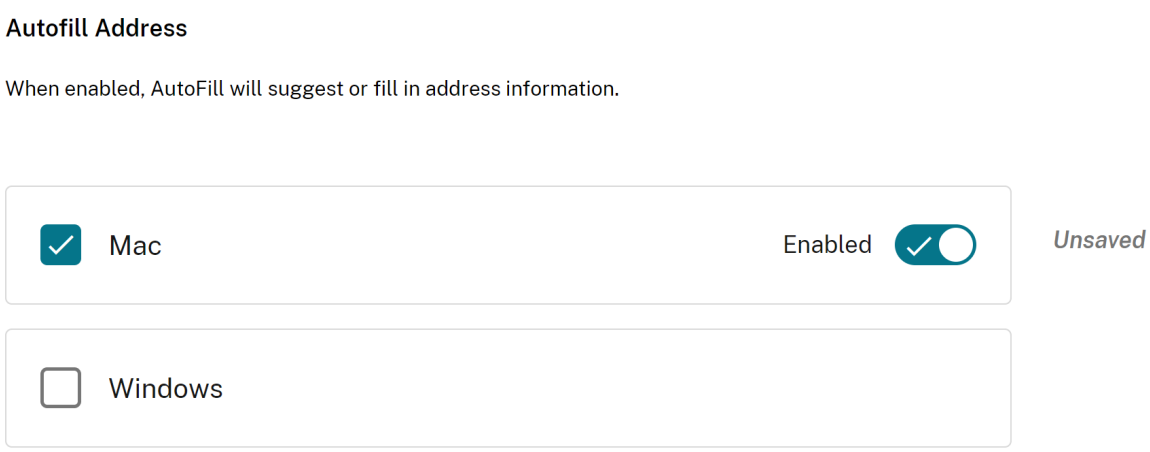


```
6   ]
7  <!--NeedCopy-->
```

> **Note:**
>
> The default value is **true**.

Configuration through UI

1. Select the appropriate operating system.
2. Enable or disable the toggle button as per your requirement.
3. Click **Publish Drafts**.
4. Click **Yes** to save the changes for your end users.



Enable autofill credit card When you enable the autofill credit card setting, autofill suggests or fills in credit card information.

Configuration through API

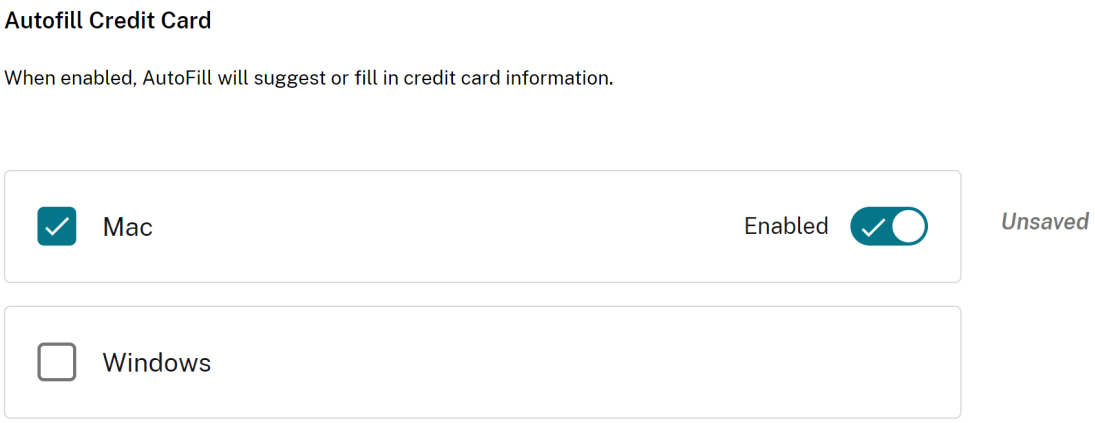
To configure, here's an example JSON file to enable autofill credit card. Setting the value to 'true' autofills the credit card details, whereas 'false'disables it.

```
1    "settings": [{
2
3         "name": "auto fill credit card enabled",
4         "value": true
5       }
6   ]
7  <!--NeedCopy-->
```

> **Note:**
>
> The default value is **true**.

Configuration through UI

1. Select the appropriate operating system.
2. Enable or disable the toggle button as per your requirement.
3. Click ***Publish Drafts**.
4. Click **Yes** to save the changes for your end users.



Auto launch protocols from origins This setting allows you to launch an external app without prompting the user for authentication. For that, add a protocol that can launch an external app and list the URLs of external apps.

Configuration through API

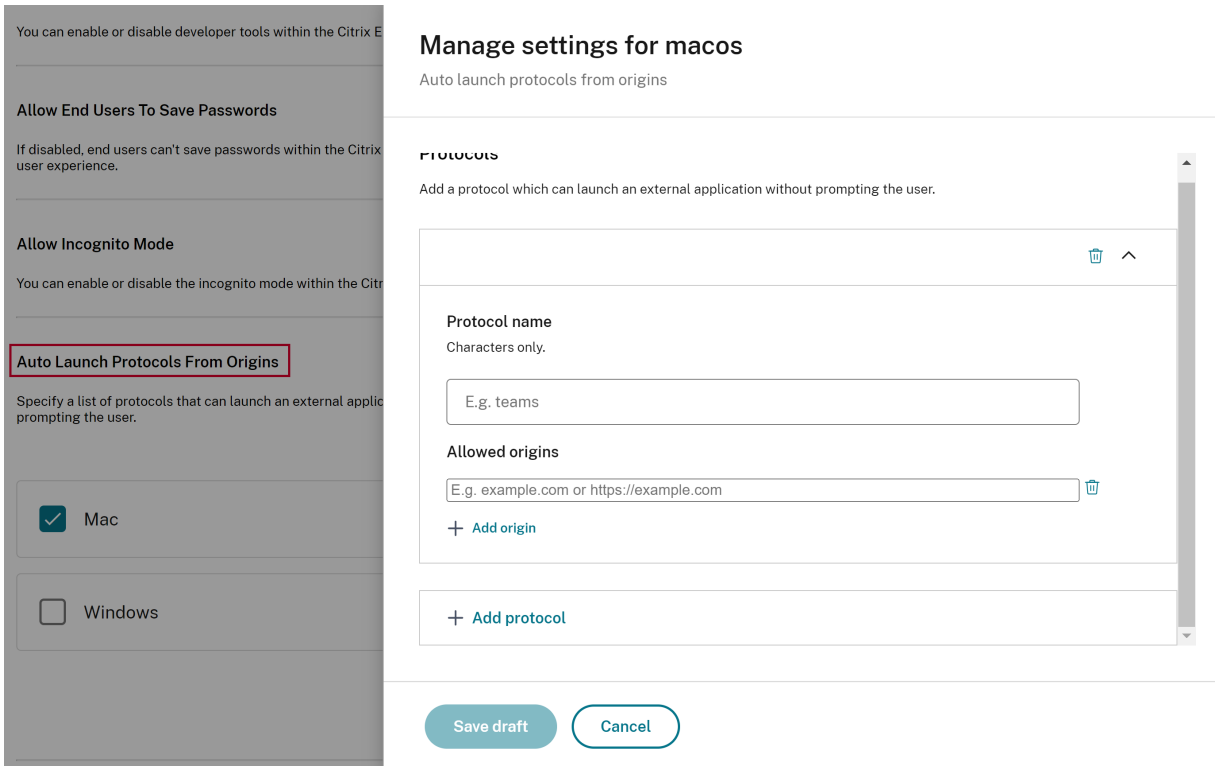
To configure, here's an example JSON file to enable this setting:

```
  "settings": [{

       "name": "auto launch protocols from origins",
       "value": [
         {

           "protocol": "teams",
           "allowed_origins": [
             "example.com",
             "http://www.example.com:8080"
           ]
          }

       ]
      }

   ]
<!--NeedCopy-->
```


> **Note:**
>
> There's no default value.

Configuration through UI

1. Select the appropriate operating system under the **Auto Launch Protocols From Origins** section.
2. Click **Edit**.
3. On the **Manage setting** screen, enter the protocol name and allowed origins.
4. Click **Save draft**.
5. On the **Save Settings** window, click **Yes** to save the settings.



Enable command-line flag security warnings You can enable this setting to display security warnings when potentially dangerous command-line flags are used to launch the browser.

Configuration through API

To configure, here's an example JSON file to enable command-line flag security warnings. Setting the value to 'true'enables the setting, whereas 'false'disables it.

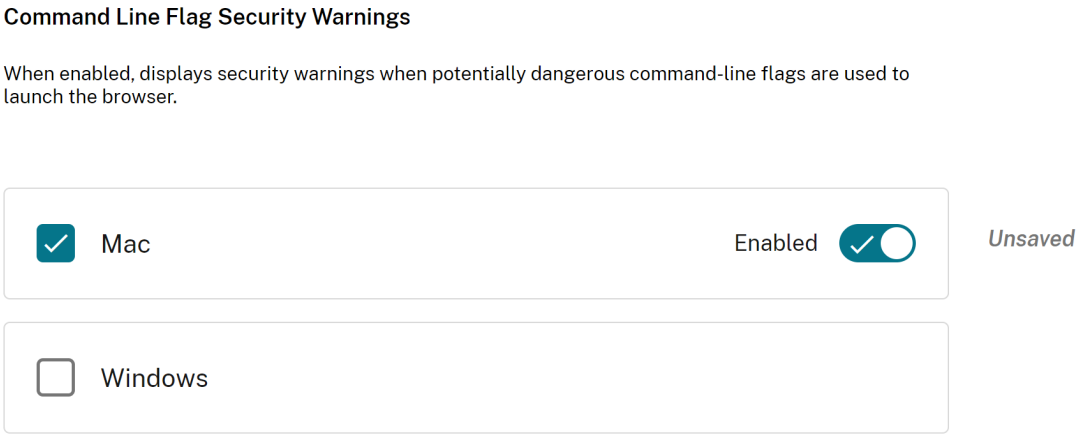
```
"settings": [{

        "name": "command line flag security warnings enabled",
        "value": true
```



```
    }
  ]
<!--NeedCopy-->
```

Configuration through UI

1. Select the appropriate operating system.
2. Enable or disable the toggle button as per your requirement.
3. Click **Publish Drafts**.
4. Click **Yes** to save the changes for your end users.



Manage default cookies setting You can enable the default cookies setting to manage how websites can store local data and cookies. Depending on your preference, you can set any of the following options:

- **Allow all sites to set local data:** This is the default setting and allows any website to store cookies and other data on your device without restriction.
- **Do not allow any site to set local data:** This setting blocks all websites from storing any cookies and local data on your device.
- **Keep cookies for the duration of the session:** This setting allows websites to store cookies while you're browsing, but deletes them once you close your browser.

Configuration through API

To configure, here's an example JSON file to enable **Default Cookies**.

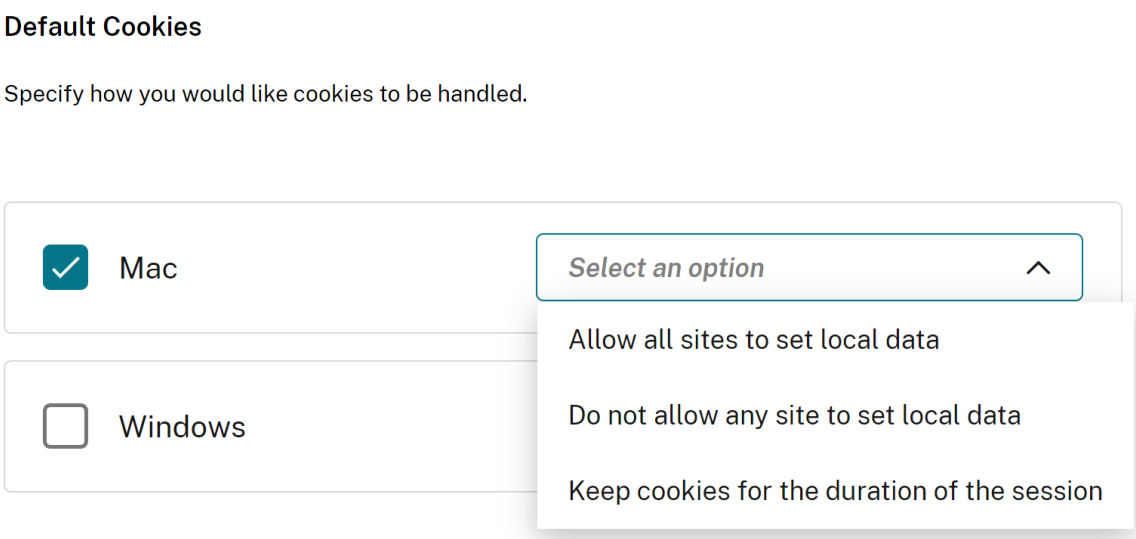
```
"settings": [{

        "name": "default cookies setting",
        "value": "Allow all sites to set local data"
    }
 ]
```



```
<!--NeedCopy-->
```

Configuration through UI

1. Select the appropriate operating system.
2. Select an option from the drop-down list.
3. Click **Publish Drafts**.
4. Click **Yes** to save the changes for your end users.



Manage default pop-ups setting You can enable the default pop-up setting to manage pop-ups from a website. Depending on your preference, you can set any of the following options:

- **Allow all sites to show pop-ups:** This is the default setting where all websites can display pop-ups.
- **BlockPopups applies, but users can change this setting:** No websites can display pop-ups. However, users can manage this setting as per their preference.
- **Do not allow any site to show pop-ups:** This setting blocks pop up from all websites.

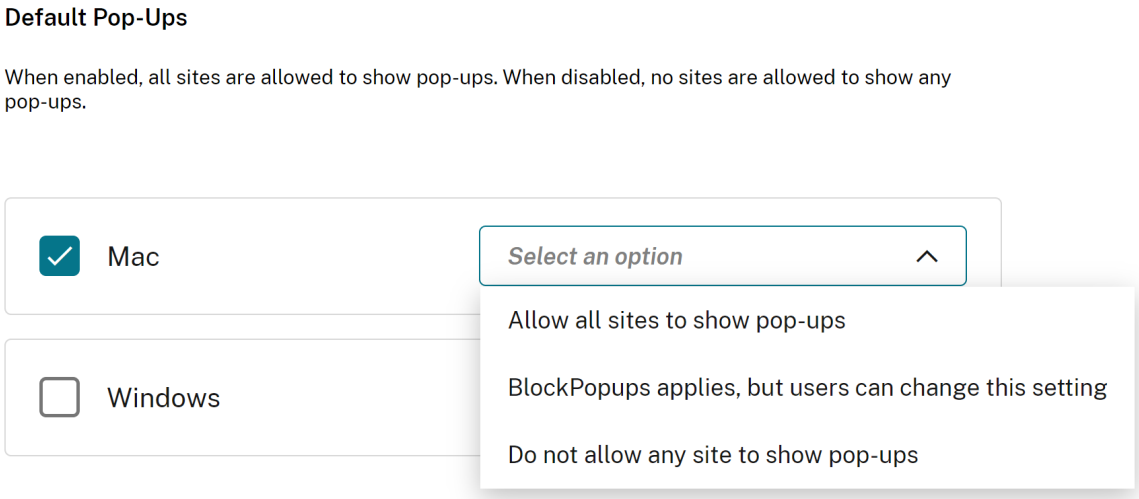
Configuration through API

To configure, here's an example JSON file to manage the default pop-up settings.

```
"settings": [{

      "name": "default popups setting",
      "value": "Allow all sites to show pop-ups"
    }
 ]
<!--NeedCopy-->
```


Configuration through UI

1. Select the appropriate operating system.
2. Select an option from the drop-down list.
3. Click **Publish Drafts**.
4. Click **Yes** to save the changes for your end users.



Extension install sources You can specify the source URLs from which users can install extensions, apps, and themes to the browser.

Configuration through API

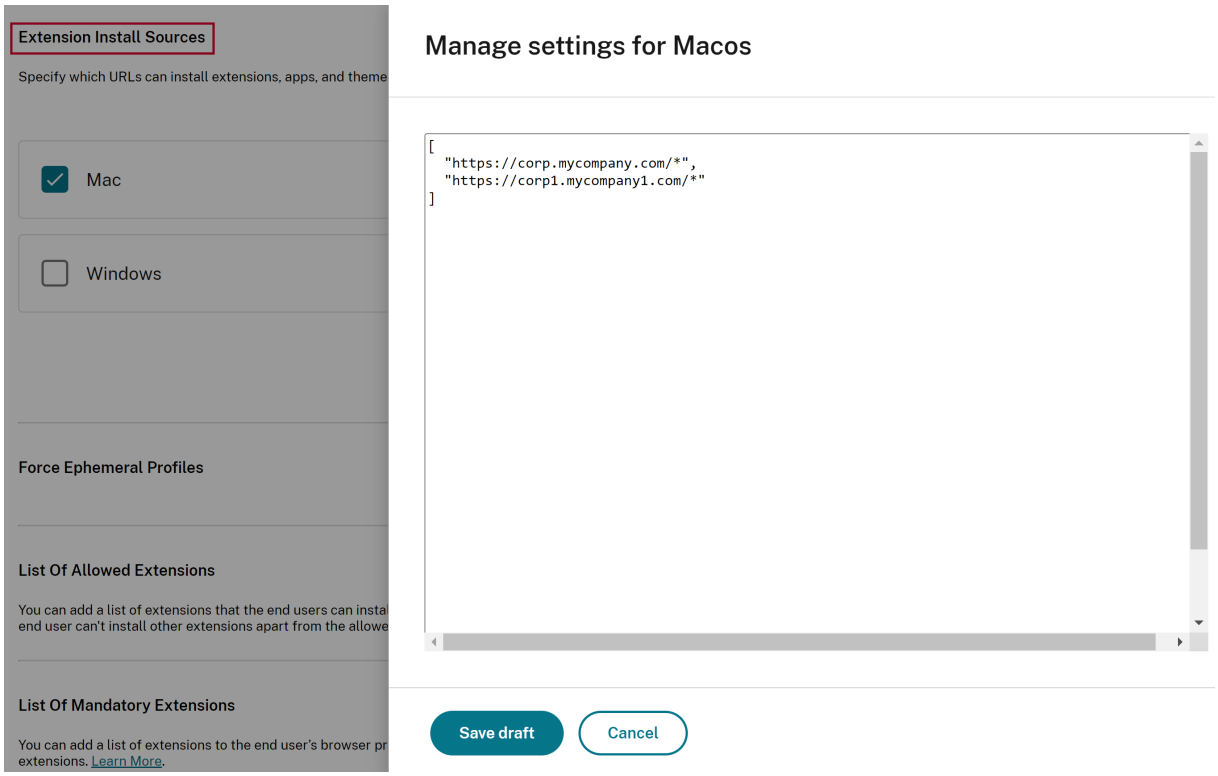
To configure, here's an example JSON file to manage this setting.

```
"settings": [{

      "name": "extension install sources",
      "value": [
          "https://corp.mycompany.com/*"
          "https://corp1.mycompany1.com/*"
        ]
   }
 ]
<!--NeedCopy-->
```

Configuration through UI

1. Select the appropriate operating system under the **Extension Install Sources** section.
2. Click **Edit**.
3. On the **Manage setting** screen, enter the list of source URLs.
4. Click **Save draft**.

5. On the **Save Settings** window, click **Yes** to save the settings.



Disable lookalike warning pages This setting allows you to prevent the display of lookalike URL warnings. If you enable the setting and specify one or more domains, no lookalike warning pages show when a user visits pages on that domain.

Configuration through API

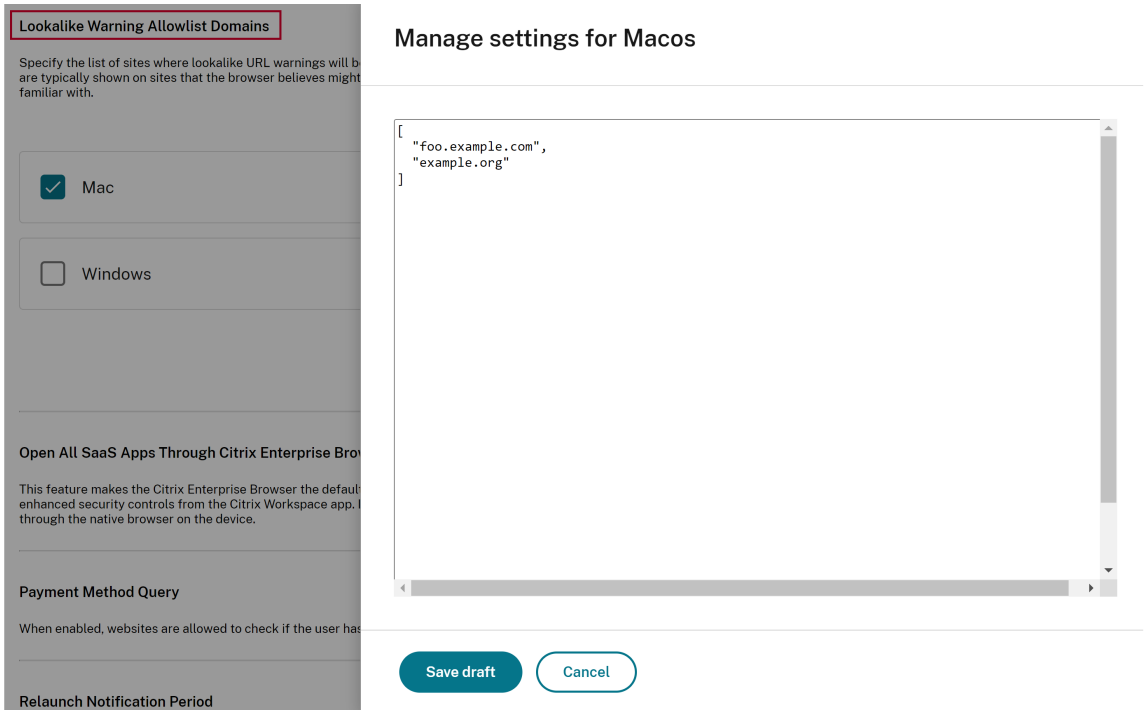
To configure, here's an example JSON file to enable this setting.

```
"settings": [{

      "name": "look alike warning allowlist domains",
      "value": [
          "foo.example.com",
          "example.org"
          ]
      }
 ]
<!--NeedCopy-->
```

Configuration through UI

1. Select the appropriate operating system under the **Lookalike Warning Allowlist Domains** section.
2. Click **Edit**.

3. On the **Manage setting** screen, enter the list of domains.
4. Click **Save draft**.
5. On the **Save Settings** window, click **Yes** to save the settings.



Enable payment method query When you enable this setting, it allows websites to check if users have saved payment methods.

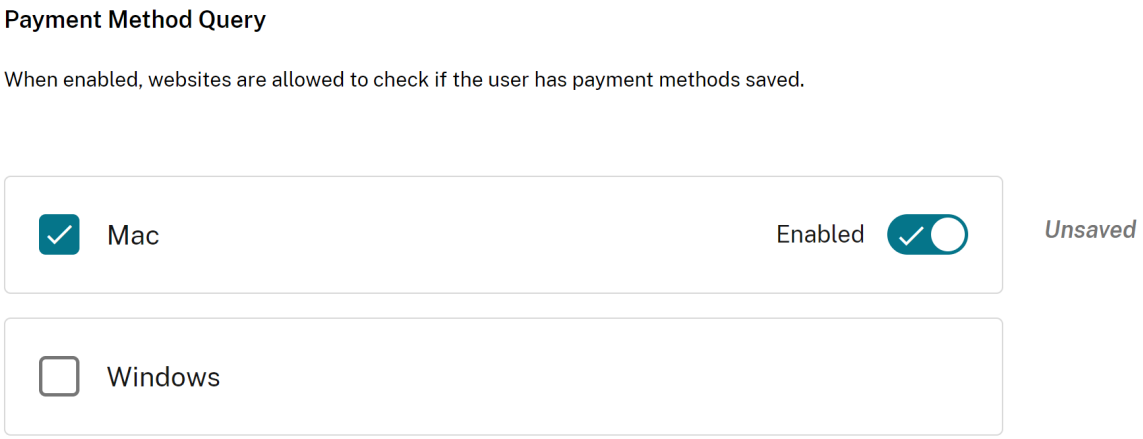
Configuration through API

To configure, here's an example JSON file to enable payment method query. Setting the value to 'true' enables this setting whereas 'false'disables it.

```
"settings": [{

      "name": "payment method query enabled",
      "value": true
   }
 ]
<!--NeedCopy-->
```

Configuration through UI

1. Select the appropriate operating system.
2. Enable or disable the toggle button as per your requirement.
3. Click **Publish Drafts**.
4. Click **Yes** to save the changes for your end users.



Manage saving browser history You can use this setting if you want to manage the saving of the browsing history.

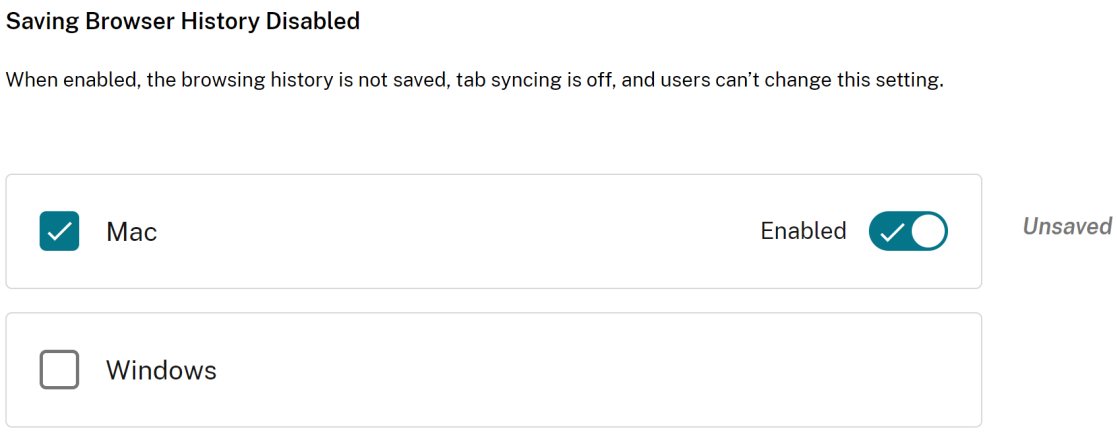
Configuration through API

To configure, here's an example JSON file to manage the saving of browser history. Setting the value to 'true'doesn't save the browsing history. The value 'false'saves the browsing history.

```
"settings": [{

      "name": "saving browser history disabled",
      "value": true
   }
 ]
<!--NeedCopy-->
```

Configuration through UI

1. Select the appropriate operating system.
2. Enable or disable the toggle button as per your requirement.
3. Click **Publish Drafts**.
4. Click **Yes** to save the changes for your end users.



Manage search suggestion You can enable this setting if you want to turn on search suggestions in the browser's address bar.

The suggestions based on the bookmarks and browser history are unaffected by this setting.

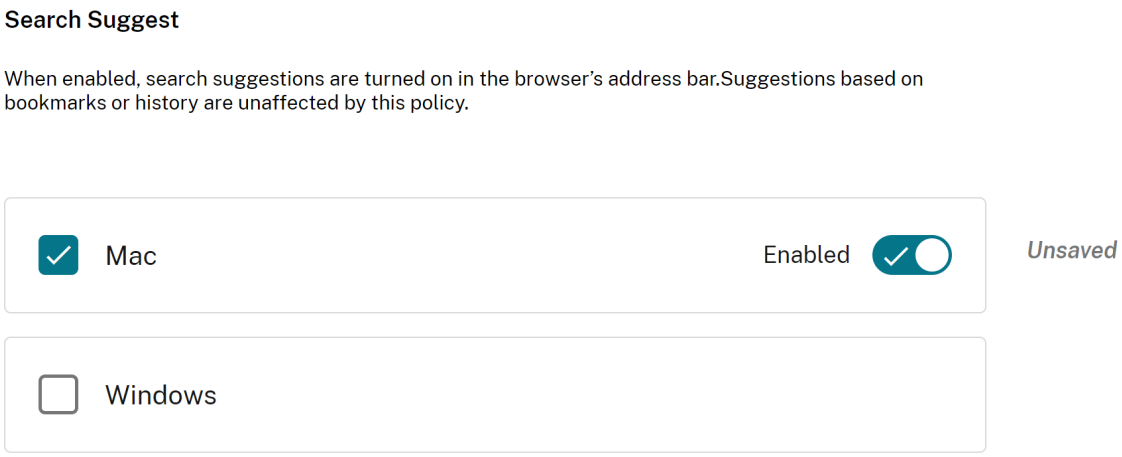
Configuration through API

To configure, here's an example JSON file to enable the search suggestions. Set the value to 'true'to turn on the search suggestions. The value 'false'turns off the search suggestions.

```
"settings": [{

      "name": "search suggest enabled",
      "value": true
   }
 ]
<!--NeedCopy-->
```

Configuration through UI

1. Select the appropriate operating system.
2. Enable or disable the toggle button as per your requirement.
3. Click **Publish Drafts**.
4. Click **Yes** to save the changes for your end users.



Enable export bookmark When you enable this setting, users can see the option to export the browser's bookmark.

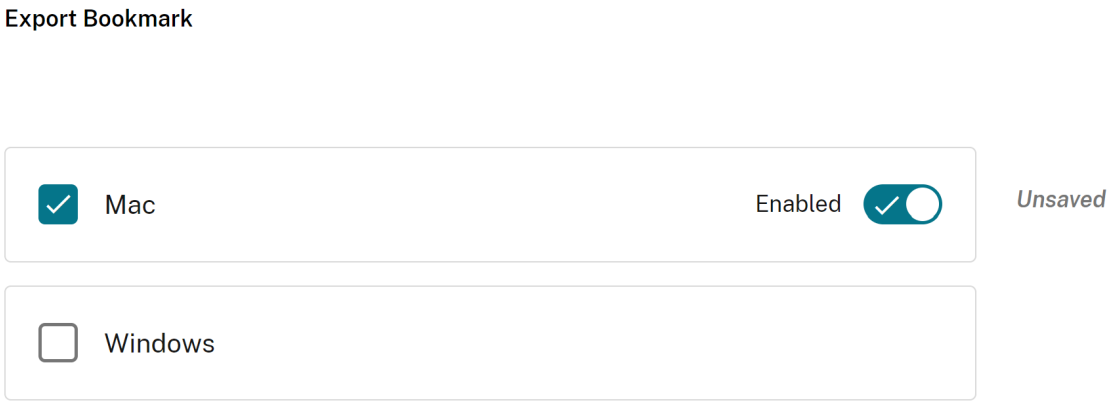
Configuration through API

To configure, here's an example JSON file to manage the exporting of browser bookmarks. Set the value to 'true'to enable the option to export the browser's bookmark. The value 'false'disables the option.

```
"settings": [{

      "name": "export bookmark allowed",
      "value": true
   }
 ]
<!--NeedCopy-->
```

Configuration through UI

1. Select the appropriate operating system.
2. Enable or disable the toggle button as per your requirement.
3. Click **Publish Drafts**.
4. Click **Yes** to save the changes for your end users.



Force ephemeral profiles When you enable this setting, it creates an ephemeral profile when users sign in to the Enterprise Browser. Ephemeral profile erases user profile data on disk when a user ends the browsing session. Users can still download files, save pages, or print them.

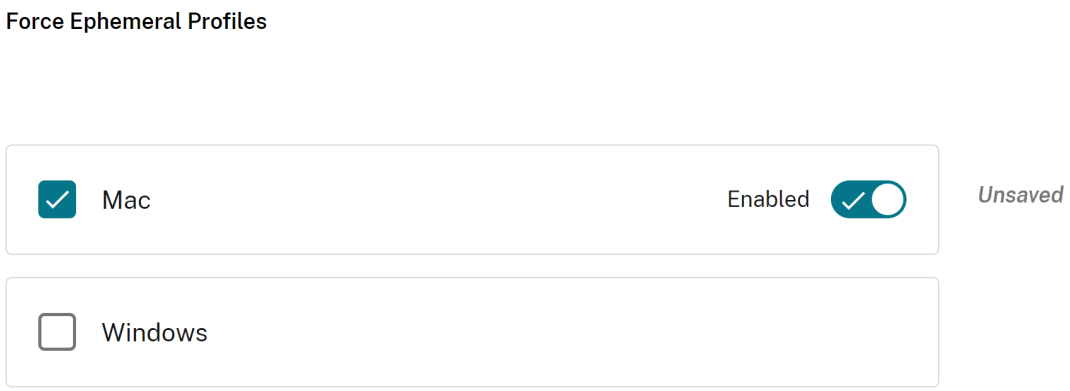
Configuration through API

To configure, here's an example JSON file to enable or disable the creation of ephemeral profiles. Set the value to 'true'to enable the setting that creates an ephemeral profile, which erases the profile data on disk when the user closes the browser. When you set the value to 'false', the profile data remains on the disk even after users end the browsing session.

```
"settings": [{

      "name": "force ephemeral profiles",
      "value": true
   }
 ]
<!--NeedCopy-->
```

Configuration through UI

1. Select the appropriate operating system.
2. Enable or disable the toggle button as per your requirement.
3. Click **Publish Drafts**.
4. Click **Yes** to save the changes for your end users.



Example JSON data The following is an example JSON file:

```
{

  "serviceURL": {

    "url": "https://example.cloudburrito.com:443"
   }
 ,
  "settings": {

    "name": "example name",
    "description": "example description",
    "useForAppConfig": true,
    "appSettings": {

      "macos": [
        {

          "category": "browser",
          "userOverride": false,
          "assignedTo": [
            "AllUsersNoAuthentication"
          ],
          "settings": [
            {

              "name": "open all apps in cwb",
              "value": true
             }
 ,
            {

              "name": "incognito mode availability",
              "value": "Incognito mode available"
             }
 ,
```



```
            {

              "name": "developer tools availability",
              "value": "Allow usage of the Developer Tools"
             }
,
            {

              "name": "enable password save",
              "value": true
             }
,
            {

              "name": "Delete browsing data on exit",
              "value": [
                "browsing_history",
                "download_history"
              ]
             }
,
            {

              "name": "Managed bookmarks",
              "value": [
                {

                  "toplevel_name": "My managed bookmarks folder"
                 }
,
                {

                  "name": "Google",
                  "url": "google.com"
                 }
,
                {

                  "name": "Youtube",
                  "url": "youtube.com"
                 }
,
                {

                  "children": [
                    {

                      "name": "Chromium",
                      "url": "chromium.org"
                     }
,
                    {

```



```
                        "name": "Chromium Developers",
                        "url": "dev.chromium.org"
                      }

                    ],
                    "name": "Chrome links"
                  }

                ]
              }
  ,
              {

                "name": "Extension Install Allow list",
                "value": [
                  {

                    "name": "test1",
                    "install link": "https://chrome.google.com/webstore/
                       detail/stayfocusd/laankejkbhbdhmipfmgcngdelahlfoji
                       ?utm_term=chrome%20web%20store&utm_campaign&
                       utm_source=adwords&utm_medium=ppc&hsa_acc
                       =2427782021&hsa_cam=17624934708&hsa_grp
                       =142148219190&hsa_ad=607700050316&hsa_src=g&
                       hsa_tgt=kwd-308053041493&hsa_kw=chrome%20web%20
                       store&hsa_mt=b&hsa_net=adwords&hsa_ver=3&gclid=
                       Cj0KCQjw852XBhC6ARIsAJsFPN2YQhvZivtPKvAX5IbRF7i4y_cEhWOSzZw
                       ",
                    "id": "laankejkbhbdhmipfmgcngdelahlfoji"
                  }
  ,
                  {

                    "name": "test2",
                    "install link": "https://chrome.google.com/webstore/
                       detail/vimium/dbepggeogbaibhgnhhndojpepiihcmeb?
                       utm_term=chrome%20web%20store&utm_campaign&
                       utm_source=adwords&utm_medium=ppc&hsa_acc
                       =2427782021&hsa_cam=17624934708&hsa_grp
                       =142148219190&hsa_ad=607700050316&hsa_src=g&
                       hsa_tgt=kwd-308053041493&hsa_kw=chrome%20web%20
                       store&hsa_mt=b&hsa_net=adwords&hsa_ver=3&gclid=
                       Cj0KCQjw852XBhC6ARIsAJsFPN2YQhvZivtPKvAX5IbRF7i4y_cEhWOSzZw
                       ",
                    "id": "dbepggeogbaibhgnhhndojpepiihcmeb"
                  }

                ]
              }
  ,
              {

                "name": "Extension Install Force list",
```

```
                "value": [
                  "ohlencieiipommannpdfcmfdpjjmeolj",
                  "dipiagiiohfljcicegpgffpbnjmgjcnf"
                ]
              }
  ,
              {

                "name": "auto fill address enabled",
                "value": true
              }
  ,
              {

                "name": "auto fill credit card enabled",
                "value": true
              }
  ,
              {

                "name": "command line flag security warnings enabled",
                "value": true
              }
  ,
              {

                "name": "payment method query enabled",
                "value": true
              }
  ,
              {

                "name": "saving browser history disabled",
                "value": true
              }
  ,
              {

                "name": "search suggest enabled",
                "value": true
              }
  ,
              {

                "name": "export bookmark allowed",
                "value": true
              }
  ,
              {

                "name": "force ephemeral profiles",
                "value": true
              }
```



```
,
            {

              "name": "default cookies setting",
              "value": "Do not allow any site to set local data"
             }
,
            {

              "name": "default popups setting",
              "value": "BlockPopups applies, but users can change this
                 setting"
             }
,
            {

              "name": "look alike warning allowlist domains",
              "value": [
                "foo.example.com",
                "example.org"
              ]
             }
,
            {

              "name": "extension install sources",
              "value": [
                "https://corp.mycompany.com/*",
                "https://corp1.mycompany1.com/*"
              ]
             }
,
            {

              "name": "auto launch protocols from origins",
              "value": [
                {

                  "protocol": "sportifys",
                  "allowed_origins": [
                    "example.com",
                    "http://www.example.com:8080"
                  ]
                 }
,
                {

                  "protocol": "teams",
                  "allowed_origins": [
                    "example1.com",
                    "http://www.example1.com:8080"
                  ]
                 }
```



```
                ]
               }

            ]
           }

       ],
       "windows": [
         {

           "category": "browser",
           "userOverride": false,
           "assignedTo": [
             "AllUsersNoAuthentication"
           ],
           "settings": [
             {

               "name": "open all apps in cwb",
               "value": true
              }
,
             {

               "name": "incognito mode availability",
               "value": "Incognito mode available"
              }
,
             {

               "name": "developer tools availability",
               "value": "Allow usage of the Developer Tools"
              }
,
             {

               "name": "enable password save",
               "value": true
              }
,
             {

               "name": "Managed bookmarks",
               "value": [
                 {

                   "toplevel_name": "My managed bookmarks folder"
                  }
,
                 {

                   "name": "Google",
```



```
282                     "url": "google.com"
283                   }
284   ,
285                   {
286
287                     "name": "Youtube",
288                     "url": "youtube.com"
289                   }
290   ,
291                   {
292
293                     "children": [
294                       {
295
296                         "name": "Chromium",
297                         "url": "chromium.org"
298                       }
299   ,
300                       {
301
302                         "name": "Chromium Developers",
303                         "url": "dev.chromium.org"
304                       }
305
306                     ],
307                     "name": "Chrome links"
308                   }
309
310                 ]
311               }
312   ,
313             {
314
315               "name": "Extension Install Allow list",
316               "value": [
317                 {
318
319                   "name": "test1",
320                   "install link": "https://chrome.google.com/webstore/
                        detail/stayfocusd/laankejkbhbdhmipfmgcngdelahlfoji
                        ?utm_term=chrome%20web%20store&utm_campaign&
                        utm_source=adwords&utm_medium=ppc&hsa_acc
                        =2427782021&hsa_cam=17624934708&hsa_grp
                        =142148219190&hsa_ad=607700050316&hsa_src=g&
                        hsa_tgt=kwd-308053041493&hsa_kw=chrome%20web%20
                        store&hsa_mt=b&hsa_net=adwords&hsa_ver=3&gclid=
                        Cj0KCQjw852XBhC6ARIsAJsFPN2YQhvZivtPKvAX5IbRF7i4y_cEhWOSzZw
                        ",
321                   "id": "laankejkbhbdhmipfmgcngdelahlfoji"
322                 }
323   ,
324                 {
325
```



```
                    "name": "test2",
                    "install link": "https://chrome.google.com/webstore/
                       detail/vimium/dbepggeogbaibhgnhhndojpepiihcmeb?
                       utm_term=chrome%20web%20store&utm_campaign&
                       utm_source=adwords&utm_medium=ppc&hsa_acc
                       =2427782021&hsa_cam=17624934708&hsa_grp
                       =142148219190&hsa_ad=607700050316&hsa_src=g&
                       hsa_tgt=kwd-308053041493&hsa_kw=chrome%20web%20
                       store&hsa_mt=b&hsa_net=adwords&hsa_ver=3&gclid=
                       Cj0KCQjw852XBhC6ARIsAJsFPN2YQhvZivtPKvAX5IbRF7i4y_cEhWOSzZwx
                       ",
                    "id": "dbepggeogbaibhgnhhndojpepiihcmeb"
                   }

                ]
              }
  ,
              {

                "name": "Extension Install Force list",
                "value": [
                  "ohlencieiipommannpdfcmfdpjjmeolj",
                  "dipiagiiohfljcicegpgffpbnjmgjcnf"
                ]
              }
  ,
              {

                "name": "Delete browsing data on exit",
                "value": [
                  "browsing_history"
                ]
              }
  ,
              {

                "name": "auto fill address enabled",
                "value": true
              }
  ,
              {

                "name": "auto fill credit card enabled",
                "value": true
              }
  ,
              {

                "name": "command line flag security warnings enabled",
                "value": true
              }
  ,
              {
```



```
370
371                 "name": "payment method query enabled",
372                 "value": true
373               }
374   ,
375               {
376
377                 "name": "saving browser history disabled",
378                 "value": true
379               }
380   ,
381               {
382
383                 "name": "search suggest enabled",
384                 "value": true
385               }
386   ,
387               {
388
389                 "name": "export bookmark allowed",
390                 "value": true
391               }
392   ,
393               {
394
395                 "name": "force ephemeral profiles",
396                 "value": true
397               }
398   ,
399               {
400
401                 "name": "default cookies setting",
402                 "value": "Do not allow any site to set local data"
403               }
404   ,
405               {
406
407                 "name": "default popups setting",
408                 "value": "BlockPopups applies, but users can change this
                      setting"
409               }
410   ,
411               {
412
413                 "name": "look alike warning allowlist domains",
414                 "value": [
415                   "foo.example.com",
416                   "example.org"
417                 ]
418               }
419   ,
420               {
421
```



```
                "name": "extension install sources",
                "value": [
                  "https://corp.mycompany.com/*",
                  "https://corp1.mycompany1.com/*"
                ]
              }
  ,
             {

                "name": "auto launch protocols from origins",
                "value": [
                  {

                    "protocol": "sportifys",
                    "allowed_origins": [
                      "example.com",
                      "http://www.example.com:8080"
                    ]
                   }
  ,
                  {

                    "protocol": "teams",
                    "allowed_origins": [
                      "example1.com",
                      "http://www.example1.com:8080"
                    ]
                   }

                ]
               }

           ]
          }

       ]
      }

    }

 }

<!--NeedCopy-->
```

Citrix Endpoint Analysis

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

> **Note:**
>
> EPA is not be installed by default.

Example: `./CitrixworkspaceApp.exe InstallEPAClient`

In this release, the EPA version packaged is 23.11.1.20.

Feature included from previous releases

This release supports features that were included in Citrix Workspace app for Windows version from 2204.1 to 2311.1 as listed below.

2311.1

The following features are added in this release:

- Introducing new installer for Citrix Workspace app
- Support for Activity Manager on cloud stores
- Automatic selection of video codec
- Loss tolerant mode for audio
- Synchronize multiple keyboards at session start
- Improved performance of BCR
- Version upgrade for Chromium Embedded Framework
- Important update on App Protection file names
- Citrix Enterprise Browser
  - Improved user experience and session reload time
  - Improved watermark design
  - Support for custom browser extension
  - Simplified SSO for Web and SaaS apps through the Global App Configuration service
  - Manage pass-through authentication in Citrix Enterprise Browser
  - Enhanced capabilities on monitoring end user activities

> **Note:**
>
> Starting with Citrix Workspace app for Windows version 2311.1, Internet Explorer-based browser content redirection is deprecated. The alternate option is to use Google Chrome-based browser content redirection.

Introducing new installer for Citrix Workspace app

The user interface of the Citrix Workspace app installer is revamped to give a modern, easy outlook, and a better user experience. By default, the new installer is enabled.

Prerequisites:

.Net Desktop Runtime 6.0.20 or later is an additional pre-requisite for the new installer. For other requirements, see System requirements section.

The new installer is enabled by default. For more information, see User interface based 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`.

Support for Activity Manager on cloud stores

Citrix Workspace app for Windows supports the Activity Manager feature. This feature lets end users view and interact with all their active apps and desktop sessions in one place. To view active sessions in the **Activity Manager**, click the **Activity Manager** icon. You can perform the following actions on an app or desktop by clicking the respective ellipsis(…) button from the Activity Manager:

- **Log out**: Logs out from the current session. All the apps in the session are closed, and any unsaved files are lost.
- **Disconnect**: The remote session is disconnected but the apps and desktops are active in the background.
- **Restart**: Shuts down your desktop and start it again.
- **Shutdown**: Closes your disconnected desktops.
- **Force quit**: Forcefully power off your desktop if there is a technical issue.
- Click the **X** button to terminate the active app session from the Activity Manager.

For more information, see Activity manager.

> **Note:**
>
> This feature is available in Citrix Workspace app for Windows only if the new Workspace experience is enabled.

Automatic selection of video codec

With this 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

This feature is enabled by default.

For more information, see Automatic selection of video codec.

H.265 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.

Starting with Citrix Workspace app 2311.1, this feature is enabled automatically with the introduction of the **Automatic selection of video codec** feature.

For more information, see the H.265 documentation.

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.

Starting with Citrix Workspace app 2311.1, this feature is enabled automatically with the introduction of the **Automatic selection of video codec** feature.

For more information, see the AV1 documentation.

Loss tolerant mode for audio

With this release, Citrix Workspace app supports Loss tolerant mode (EDT lossy) 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.

For more information, see the Loss tolerant mode for audio documentation.

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.

With this 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.

For more information, see the Synchronize multiple keyboards at session start documentation.

Improved performance of BCR

Previously, BCR used client-side disk space cache and the cached information wasn't deleted during an upgrade. This setting resulted in higher disk space usage over time and inconsistent behavior while a page is redirected using BCR.

With this release, to resolve this issue, BCR uses an in-memory cache. This enhancement helps to improve the performance of BCR.

This feature is disabled by default.

For more information, see Improved performance of BCR.

Version upgrade for Chromium Embedded Framework

The version of the Chromium Embedded Framework (CEF) is upgraded to 117. This version upgrade helps to resolve security vulnerabilities.

Important update on App Protection file and driver names

Starting with Citrix Workspace app for Windows 2311.1, the following file and driver names are updated as follows:

Existing name	New name
`EntryProtect.dll`	`ctxapdotnet.dll`
`entryprotect.sys`	`ctxapdriver.sys`
`epclient32.dll`	`ctxapclient32.dll`
`epclient64.dll`	`ctxapclient64.dll`
`epinject.sys`	`ctxapinject.sys`
`epusbfilter.sys`	`ctxapusbfilter.sys`
`entryprotectdrv`	`ctxapdriver`
`epinject6`	`ctxapinject`

These files are installed at `%ProgramFiles(x86)%\Citrix\ICA Client` by default.

If you've added any of the preceding file or driver names to the allow list in your environment, update the allow list.

Enhancement to background blurring and effects for Microsoft Teams optimization with HDX

Starting with Citrix Workspace app version 2311.1, you can select the following options for background blurring and effects:

- No background effect
- Select Background Blurring
- Select Background Image

Citrix Enterprise Browser

This release includes Citrix Enterprise Browser version 119.1.1.60, based on Chromium version 115. For more information about the Citrix Enterprise Browser, see the Citrix Enterprise Browser documentation.

Citrix Enterprise Browser introduces additional settings in the Global App Configuration service
Additional settings have been added into the Global App Configuration service (GACS) for configuring Citrix Enterprise Browser. For more information, see Manage Citrix Enterprise Browser through GACS.

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 is 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.

Improved user experience Previously, Citrix Enterprise Browser displayed a reconnection modal when you attempted to perform an action after your session expired. Starting with Citrix Workspace app for Windows version 2311.1 (which corresponds to the Chromium version 119.1.1.60), there is no longer a reconnection modal. Instead, a loading icon now appears on the browser tab when you attempt to perform any action after your session expires.

Improved watermark design Citrix Enterprise Browser now has a new watermark design that is less intrusive and provides a better user experience.

Support for custom browser extension Citrix Enterprise Browser has expanded its extension capabilities. Previously, only extensions from the Chrome Web Store were permitted. Citrix Enterprise Browser now allows you to add custom extensions securely. Administrators can configure custom extensions as part of the mandatory list. End users can access and use these extensions either via `citrixbrowser://extensions` or by clicking the **Extensions** option under the **More** button as needed. For more information on how to configure the custom extensions, see Mandatory custom extension.

Simplified SSO for Web and SaaS apps through the Global App Configuration service Previously, single sign-on (SSO) was configured for Citrix Enterprise Browser using the PowerShell module. Now, this simplified SSO feature allows you to configure SSO in Citrix Enterprise Browser by using a newly introduced setting in the Global App Configuration service (GACS). Administrators can use this new setting to enable SSO for all web and SaaS apps in Citrix Enterprise Browser. This method eliminates the need for the complex PowerShell module. For more information on how to manage SSO through GACS, see Manage single sign-on for Web and SaaS apps through the Global App Configuration service.

> **Note:**
>
> We recommend you to restart Citrix Workspace app when you modify the Citrix Enterprise Browser settings in GACS. However, you can also wait for the automatic refresh to complete. For more information on the sync duration of policies fetched from GACS, refer Frequency of settings update.

Extending simplified single sign-on functionality to StoreFront The single sign-on (SSO) feature is now available for StoreFront, which assures a unified SSO experience. This new capability eliminates the need for users to authenticate separately when accessing apps through StoreFront. To facilitate this SSO feature, use the same Identity Provider (IdP) for both Web and SaaS apps, and for StoreFront. For more information on how to manage SSO through GACS, see Manage single sign-on for Web and SaaS apps through the Global App Configuration service.

Manage pass-through authentication in Citrix Enterprise Browser Pass-through authentication (PTA) is a feature of Azure AD Connect. PTA is an authentication method where the user credentials are passed from the client machine to the server. You never see it as it happens on the back end. In this method, the client machine directly communicates with the authentication server to validate the user's credentials. PTA is typically used when your client machine and the authentication server trust each other, and your client machine is considered to be secure. For more information on Microsoft Azure AD pass-through authentication, see Microsoft Entra seamless single sign-on.

To facilitate pass-through authentication, you need the Windows Accounts extension to interact with applications that require Azure AD-based access within the Enterprise Browser. Administrator need to configure this Windows Accounts extension as part of the mandatory list under **ExtensionInstallForcelist**. For more information on the configuration of mandatory extensions, see Mandatory extension.

Enhanced capabilities on monitoring end user activities Previously, administrators were unable to monitor end user activities such as App accessed and Traffic type. Starting with Citrix Workspace app for Windows 2311.1 (corresponding to Chromium version 119.1.1.60), you can now monitor these details as well.

- **App accessed**: Enterprise Browser provides information about all the apps accessed by the end user, provided the app is listed in the policy document.
- **Traffic type**: Enterprise Browser provides information about whether data is sent directly or through Secure Private Access authentication.

To monitor the end user activities from the Enterprise Browser, use the Citrix Analytics service using your Citrix Cloud account. After signing in to Citrix Cloud, navigate to **Analytics > Security > Search**. There, you can refer to **Apps and Desktops** under the **Self-Service Search** section. For more information on Citrix Analytics, see Getting started.

2309.1

What's new

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

Citrix Enterprise Browser

This release includes Citrix Enterprise Browser version 117.1.1.13, based on Chromium version 117. For more information about the Citrix Enterprise Browser, see the Citrix Enterprise Browser documentation.

2309

What's new

> **Note:**
>
> From this release onwards, ensure that the Microsoft Edge WebView2 Runtime version is 117 or later. We recommend you to install the latest version to get newer functionalities and security-related fixes.

The following features are added in this release:

- Additional .NET prerequisites
- Improved virtual apps and desktops launch experience
- Addition of the Troubleshooting option in the system tray of Citrix Workspace app
  - Send feedback on Citrix Workspace app
- Sustainability initiative from Citrix Workspace app
- Configure keyboard layout synchronization using command-line interface

- Command to cleanup and install Citrix Workspace app
- App Protection
  - Important update on file names
  - Policy tampering detection
  - App Protection with DoubleHop scenario
- Citrix Enterprise Browser
  - Authentication through Citrix Enterprise Browser

Additional .NET prerequisites In addition to .NET Framework 4.8, Citrix Workspace app requires the x86 version of.NET Desktop Runtime 6.0 for both x86 and x64 systems with admin privileges. For more information, see .NET requirements.

Improved virtual apps and desktops launch experience

> **Note:**
>
> From Citrix Workspace app version 2305.1 and later, 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 isn't 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 feature helps to keep the users engaged with timely and relevant information about the launch status.

For more information, see Improved virtual apps and desktops launch experience.

Addition of the Troubleshooting option in the system tray of Citrix Workspace app 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.

For more information, see Addition of the Troubleshooting option in the system tray of Citrix Workspace app.

Sustainability initiative from Citrix Workspace app When this feature is enabled, a prompt appears 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.

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

Commands to configure keyboard layout synchronization using command-line interface Previously, you could configure keyboard layout synchronization using the GUI or by updating the configuration file only. With this release, the new commands are introduced to configure keyboard layout synchronization using the command-line-interface.

For more information, see Configure keyboard layout synchronization using command-line interface.

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
<!--NeedCopy-->
```

Optimized Microsoft Teams updates

Upcoming Microsoft Teams Single-Window EOL On January 31, 2024, Microsoft will retire the Microsoft Teams support for Single-window UI when using VDI Microsoft Teams optimization and support only the Multi-Window experience. You must use a version of Citrix Virtual Apps and Desktops and Citrix Workspace app that support the Multi-Window feature to continue using certain optimized Microsoft Teams functionalities. For more information, see Upcoming Microsoft Teams Single-Window EOL.

Deprecation announcement of the SDP format (Plan B) from WebRTC Citrix is planning to deprecate the current SDP format (Plan B) support from WebRTC in future releases. You must use a version of Citrix Workspace app that supports the Unified Plan to continue using certain optimized Microsoft Teams functionalities. For more information, see Deprecation announcement of the SDP format (Plan B) from WebRTC.

App Protection

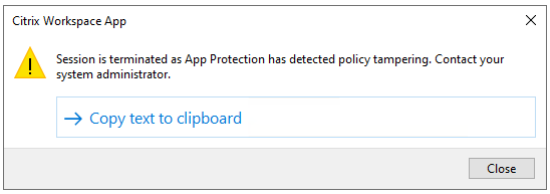
Important update on file names In a future release for Citrix Workspace app for Windows, the following file names will be updated as follows:

Existing file name	New file name
`EntryProtect.dll`	`ctxapdotnet.dll`
`entryprotect.sys`	`ctxapdriver.sys`
`epclient32.dll`	`ctxapclient32.dll`
`epclient64.dll`	`ctxapclient64.dll`
`epinject.sys`	`ctxapinject.sys`
`epusbfilter.sys`	`ctxapusbfilter.sys`
`entryprotectdrv`	`ctxapdriver`
`epinject6`	`ctxapinject`

These files are installed at `%ProgramFiles(x86)%\Citrix\ICA Client` by default.

If you've added any of the preceding file names to the allow list in your environment, update the allow list.

Policy tampering detection Policy tampering detection feature prevents the user from accessing the Virtual App or Desktop session if the App Protection anti-screen capture and anti-keylogging policies are tampered. If policy tampering is detected, the virtual app or desktop session will be terminated displaying the following error message:



> **Note:**
>
> This feature will be available only after the release of the upcoming version of Citrix Virtual Apps and Desktops.

For more information about the policy tampering detection feature, see Policy tampering detection.

Full desktop sharing capability from the VDA with Citrix Workspace app Previously when App Protection is enabled, desktop sharing is disabled for Optimized Microsoft Teams as App Protection doesn't allow you to capture the screen.

From Citrix Workspace app for Windows 2309 version and later, desktop sharing is enabled for Optimized Microsoft Teams even if App Protection is enabled.

For more information, see Compatibility with HDX optimization for Microsoft Teams.

App Protection with DoubleHop scenario App Protection features aren't supported in a double hop scenario. Double hop means a Citrix Virtual Apps or Virtual Desktops session running within a Citrix Virtual Desktops session. You were allowed to launch virtual apps and desktops enabled with App Protection policies in a double hop scenario. However, the App Protection features weren't applied.

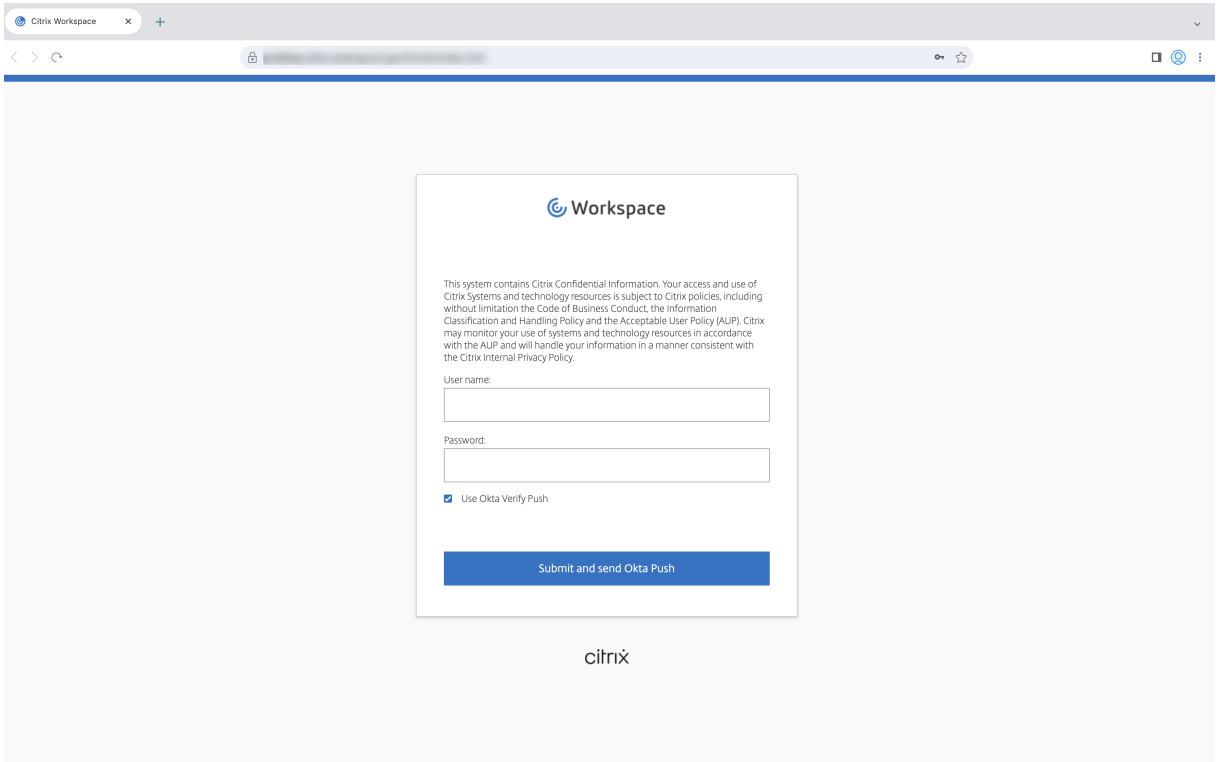
Now, a Windows Group Policy is introduced which allows you to block opening virtual apps and desktops enabled with App Protection policies in a double hop scenario. For more information about enabling the **Block DoubleHop Launch** setting, see Enable Block DoubleHop Launch setting.

Citrix Enterprise Browser This release includes Citrix Enterprise Browser version 117.1.1.9, based on Chromium version 117. For more information about the Citrix Enterprise Browser, see the Citrix Enterprise Browser documentation.

Authentication through Citrix Enterprise Browser Previously, if the authentication token for Citrix Workspace app expired, you weren't able to use the Enterprise Browser. You had to switch to Citrix Workspace app and reauthenticate to continue using the Enterprise Browser.

Starting with the Citrix Workspace app for Windows 2309 version (which corresponds to the Chromium version 117.1.1.9), you can authenticate within the Enterprise Browser itself only when the store remains the same. It ensures authentication to Citrix Workspace app as well. In addition, this feature provides a seamless login experience.

> **Note:**
>
> - This feature applies to Workspace stores.



2307.1

What's new

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

2307

What's new

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.

With this 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.

> **Note:**
>
> The preceding feature is available only after the roll-out of a corresponding update from Microsoft Teams. Check the documentation update and the announcement in CTX253754.

Citrix Enterprise Browser This release includes Citrix Enterprise Browser version 112.1.1.24, based on Chromium version 112. For more information about the Citrix Enterprise Browser, see the Citrix Enterprise Browser documentation.

Citrix Enterprise Browser shortcut Starting with the Citrix Workspace app for Windows 2307 version, an administrator can configure and control the presence of the Citrix Enterprise Browser shortcut on the **Start** menu.

> **Note:**
>
> By default, this setting is enabled for Workspace stores.

Configuration An IT administrator can configure the presence of the Citrix Enterprise Browser shortcut in one of the following ways:

- Group Policy Object (GPO)
- Global App Configuration Service (GACS)
- web.config.file.

> **Notes:**
>
> - All the configuration methods have equal priority. Enabling any one of them enables the shortcut.
> - If you haven't configured the shortcut but have one or more Workspace stores, the shortcut gets automatically enabled.
> - For end users, the Citrix Enterprise Browser shortcut appears if the user makes it as a favorite app irrespective of the configuration.
> - To disable this feature for Workspace stores, administrators must apply the following settings in any one of the following:
>   - set the **CEBShortcutEnabled** attribute to **false** in the `web.config` file.
>   - disable the **Enable Citrix Enterprise Browser shortcut** property in GPO and GACS.

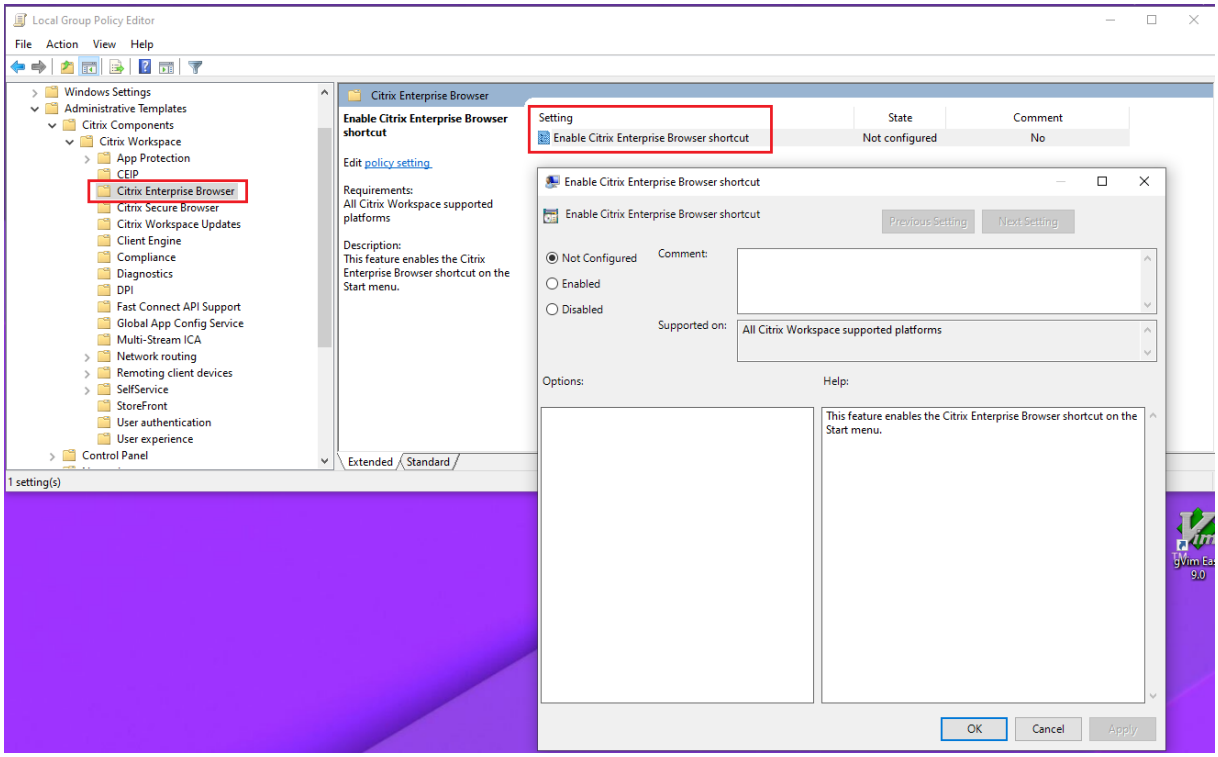
Using Group Policy Object

Administrators can use the **Enable Citrix Enterprise Browser shortcut** property to control the display of the Citrix Enterprise Browser shortcut on the Start menu.

> **Note:**
>
> Configuration through GPO is applicable on Workspace and StoreFront.

To enable the Citrix Enterprise Browser shortcut, 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** > **Citrix Enterprise Browser**.
3. Select the **Enable Citrix Enterprise Browser** shortcut option.



For more information on how to use the GPO, see the Group Policy Object administrative template page.

Global App Configuration service (GACS)

Navigate to **Workspace Configuration** > **App Configuration** > **Citrix Enterprise Browser** and enable **Enable Citrix Enterprise Browser shortcut**.

For more information on how to use the GACS UI, see the User interface article in the Citrix Enterprise Browser documentation.

> **Note:**
>
> This way of configuration is applicable on Workspace and StoreFront.

web.config file:

Enable the attribute **CEBShortcutEnabled** under the properties.

```
<properties>

            <property name="CEBShortcutEnabled" value="True" />

</properties>
<!--NeedCopy-->
```

> **Note:**
>
> Configuration through `web.config` is applicable on StoreFront.

Using web.config:

To enable the Citrix Enterprise Browser shortcut, do the following:

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">`
3. Before the `</account>` tag, navigate to the properties of that user account and add the following:

   ```
   <properties>

           <property name="CEBShortcutEnabled" value="True" />

   </properties>
   <!--NeedCopy-->
   ```

Following is an example of the `web.config` file:

```
<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="CEBShortcutEnabled" value="True
                              " />
                 </properties>
             </metadata>
        </annotatedServiceRecord>
</annotatedServices>
<metadata>
           <plugins>
                   <clear />
           </plugins>
          <trustSettings>
                       <clear />
          </trustSettings>
          <properties>
                 <clear />
          </properties>
       </metadata>
</account>

<!--NeedCopy-->
```

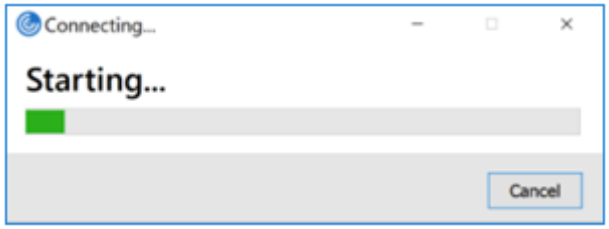
2305.1

What's new

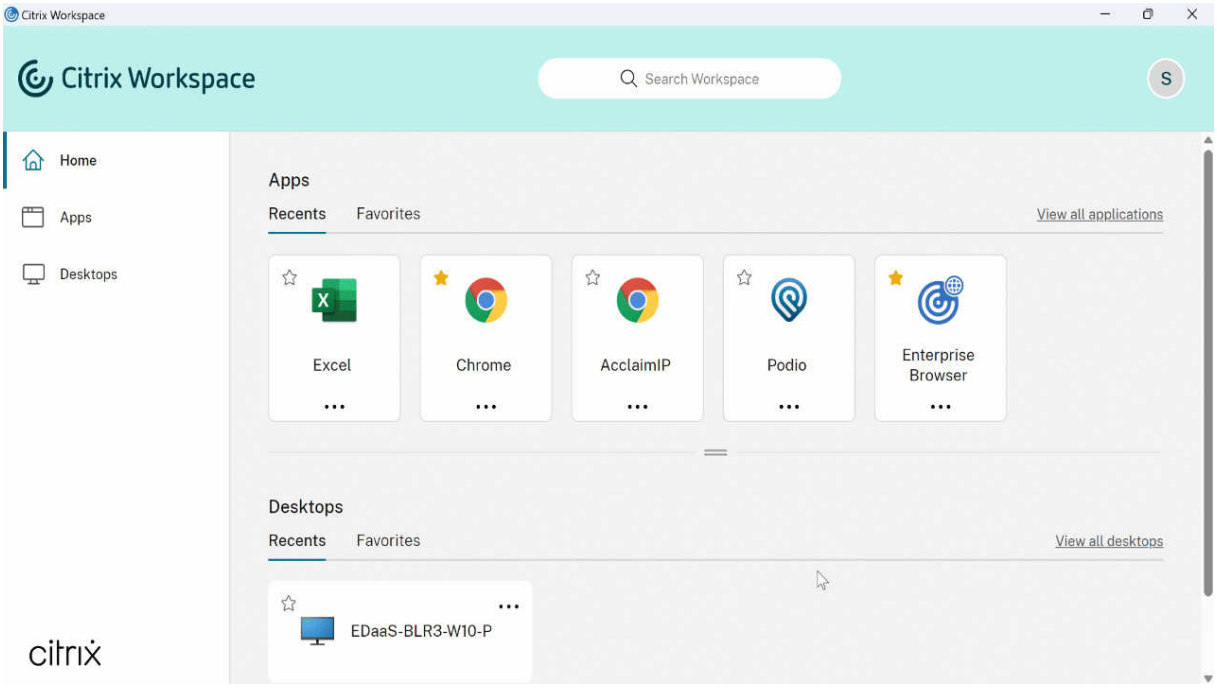
Improved virtual apps and desktops launch experience

> **Note:**
>
> This feature is generally available for cloud stores and it is in technical preview 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 isn't 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 feature 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.



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 sessions.

You can enable this feature using the registry key for the StoreFront (on-premises) session. For more information, see Improved virtual apps and desktops launch experience.

Tracking Storebrowse command status 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 store0-5
    c3ec017 -CitrixID store0-5c3ec017@@a9a8e3ac-099d-4577-b84e-
    e33d0695df39.Notepad -ica "https://cwawiniwstest.cloudburrito.com/
    Citrix/Store/resources/v2/
    YTlhOGUzYWMtMDk5ZC00NTc3LWI4NGUtZTMzZDA2OTVkZjM5Lk5vdGVwYWQ-/launch/
    ica" -cmdline

<!--NeedCopy-->
```

Support for modern authentication methods for StoreFront stores Citrix Workspace app 2305.1 for Windows support modern authentication methods for StoreFront stores. 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 102 or later.

You can enable modern authentication methods for StoreFront stores using the Global App Config service and Group Policy Object (GPO) template. For more information, see the Support for modern authentication methods for StoreFront stores section.

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.

App Protection

Enhancement on anti-keylogging With this enhancement, anti-keylogging is enabled on the authentication and self-service plug-in (SSP) screens if one of the following criteria is met:

- You have enabled App Protection using one of the following:
  - Select the **Start App Protection** checkbox during installation.
  - Start the App Protection component using the `startappprotection` command line parameter.
- If you haven't selected the **Start App Protection** checkbox or used the `startappprotection` command line parameter during the installation, then the anti-keylogging protection is enabled after launching the first protected resource.

> **Note:**
>
> The Global App Configuration service (GACS) and Group policy objects (GPO) settings override the preceding behavior. For example, if you've disabled the GACS or GPO policy for these screens, the anti-keylogging is not enabled on the authentication and SSP screens.

Important update on file names In a future release for Citrix Workspace app for Windows, the following file names will be updated:

- EntryProtect.dll
- entryprotect.sys
- epclient32.dll
- epclient64.dll
- epinject.sys
- epusbfilter.sys
- entryprotectdrv
- epinject6

These files are installed at `%ProgramFiles(x86)%\Citrix\ICA Client\`.

If you've added any of these file names to the allow list in your environment, update the allow list when the new file names are announced.

Citrix Enterprise Browser This release includes Citrix Enterprise Browser version 105.1.1.27, based on Chromium version 105. For more information about the Citrix Enterprise Browser, see the Citrix Enterprise Browser documentation.

Support for browser extensions You can add extensions that are provided by your administrator to the Citrix Enterprise Browser in a secure way. An administrator can deploy, manage, and control the extensions. End users can view and use the extension under `citrixbrowser://extensions` as required. For more settings, see Global App Configuration Service.

For more information on how to configure, see Support for browser extensions.

Modification in SPA policy implementation on internal Web and SaaS apps This feature enhances the security policies implementation on Web and SaaS apps. When a webpage and iframes within the webpage have different policies, we now have a stricter policy implementation where a union of all policies is applied on the entire webpage, including the iframes. However, the watermark is applied to the webpage only.

Use the Global App Config service to manage Citrix Enterprise Browser The administrator can use the Global App Configuration service (GACS) for Citrix Workspace to deliver Citrix Enterprise Browser settings through a centrally managed service.

The Global App Configuration service is designed for administrators to easily configure Citrix Workspace and manage the Citrix Workspace app settings. This feature allows admins to use the Global App Configuration Service to apply various settings or system policies to the Citrix Enterprise Browser on a particular store. The administrator can now configure and manage the following Citrix Enterprise Browser settings using APIs or the GACS Admin UI:

- "Enable CEB for all apps"- Makes the Citrix Enterprise Browser the default browser for opening web and SaaS apps from the Citrix Workspace app.
- "Enable save passwords"- Allow or deny end users the ability to save passwords.
- "Enable incognito mode"- Enable or disable incognito mode.
- "Managed Bookmarks"- Allow an administrator to push bookmarks to the Citrix Enterprise Browser.
- "Enable developer tools"- Enable or disable developer tools within the Enterprise Browser.
- "Delete browsing data on exit"- Allow the administrator to configure what data the Citrix Enterprise Browser deletes on exit.

- "Extension Install Force list"- Allow the administrator to install extensions in the Citrix Enterprise Browser.
- "Extension Install Allow list"- Allow the administrator to configure an allowed list of extensions that users can add to the Citrix Enterprise Browser. This list uses the Chrome Web Store.

For more information, see Use Global App Configuration service to manage Citrix Enterprise Browser.

> **Notes:**
>
> - The name and value pair are case-sensitive.
> - All the browser settings in Global App Configuration Service are under the following categories:

```
{

    "category": "browser",
    "userOverride": false,
    "assignedTo": [
    "AllUsersNoAuthentication"
    ]
 }


<!--NeedCopy-->
```

> - The administrator can apply the settings to unmanaged devices as well. For more information, see the Global App Configuration Service documentation.

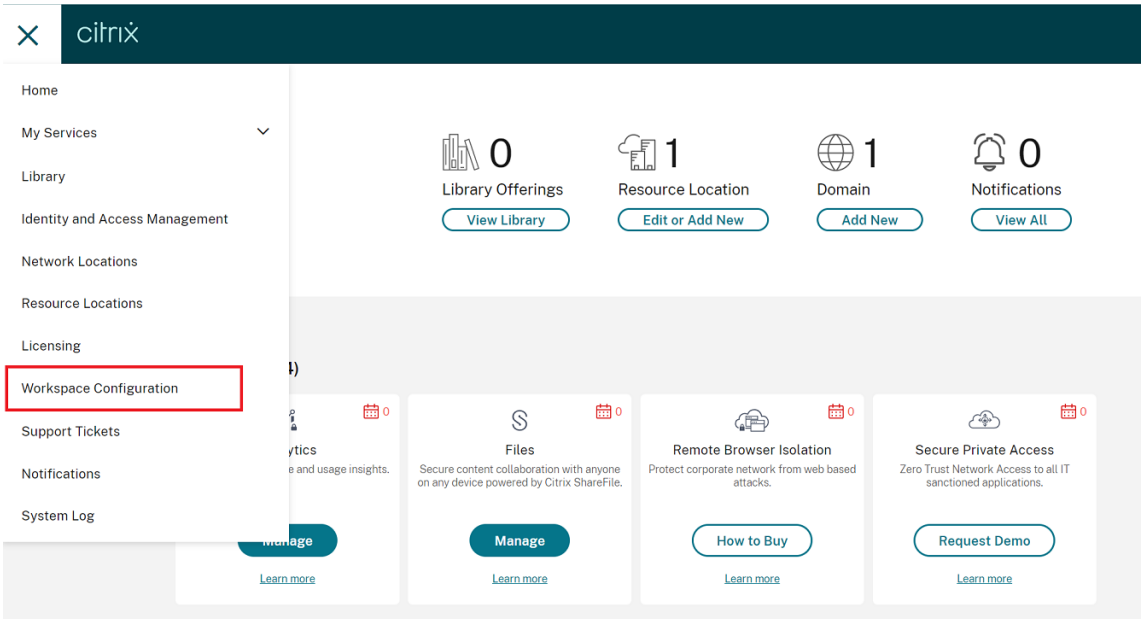
User interface

To configure Citrix Enterprise Browser 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 **Workspace Configuration**.



The **Workspace Configuration** screen appears.

3. Click **App Configuration** > **Citrix Enterprise Browser**.

   You can now configure, modify, and publish Citrix Enterprise Browser feature settings.

For more information, see Use Global App Configuration service to manage Citrix Enterprise Browser.

2303

What's new

Configure path for Browser Content Redirection overlay Browser temp data storage Starting with Citrix Workspace app 2303 version, you are requested to configure temp data storage path for the Chromium Embedded Framework (CEF) based browser.

For more information, see Configure path for Browser Content Redirection overlay Browser temp data storage.

Support for modern authentication methods for StoreFront stores Citrix Workspace app 2303 for Windows support modern authentication methods for StoreFront stores. 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 102 or later.

You can enable modern authentication methods for StoreFront stores using the GPO template. For more information, see the Support for modern authentication methods for StoreFront stores section.

Improved experience for optimized Microsoft Teams video conference calls Starting with this 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.

> **Note:**
>
> This feature is available only after the roll-out of an update from Microsoft Teams. For information on ETA, go to https://www.microsoft.com/ and search for the Microsoft 365 roadmap. When the update is rolled-out by Microsoft, you can check CTX253754 for the documentation update and the announcement.

Enhancement to App Protection: Anti-DLL Injection As part of App Protection, we now have a security enhancement that helps to protect the Citrix Workspace app from certain unauthorized dynamic-link libraries (DLL) or untrusted modules. If such untrusted modules are injected, the Citrix Workspace app detects these interventions and stops the modules from loading.

The anti-DLL injection can be enabled for the following components:

- Citrix Auth Manager
- Citrix Workspace app UI
- Citrix Virtual Apps and Desktops

For more information, see the App Protection documentation.

> **Disclaimer:**
>
> This capability works by filtering access to required functions of the underlying operating system (specific API calls required to load DLLs). Doing so means that it can provide protection even against certain custom and purpose-built hacker tools. However, as operating systems evolve, new ways of loading DLLs can emerge. While we continue to identify and address them, we cannot guarantee full protection in specific configurations and deployments.

Citrix Enterprise Browser This release includes Citrix Enterprise Browser version 109.1.1.29, based on Chromium version 109. For more information about the Citrix Enterprise Browser, see the Citrix Enterprise Browser documentation.

Secure Private Access support for StoreFront As an administrator, you can now configure Web and SaaS apps in StoreFront using a Secure Private Access solution. After the administrator configures the app, end users can open the Web and SaaS apps using Citrix Enterprise Browser with enhanced security.

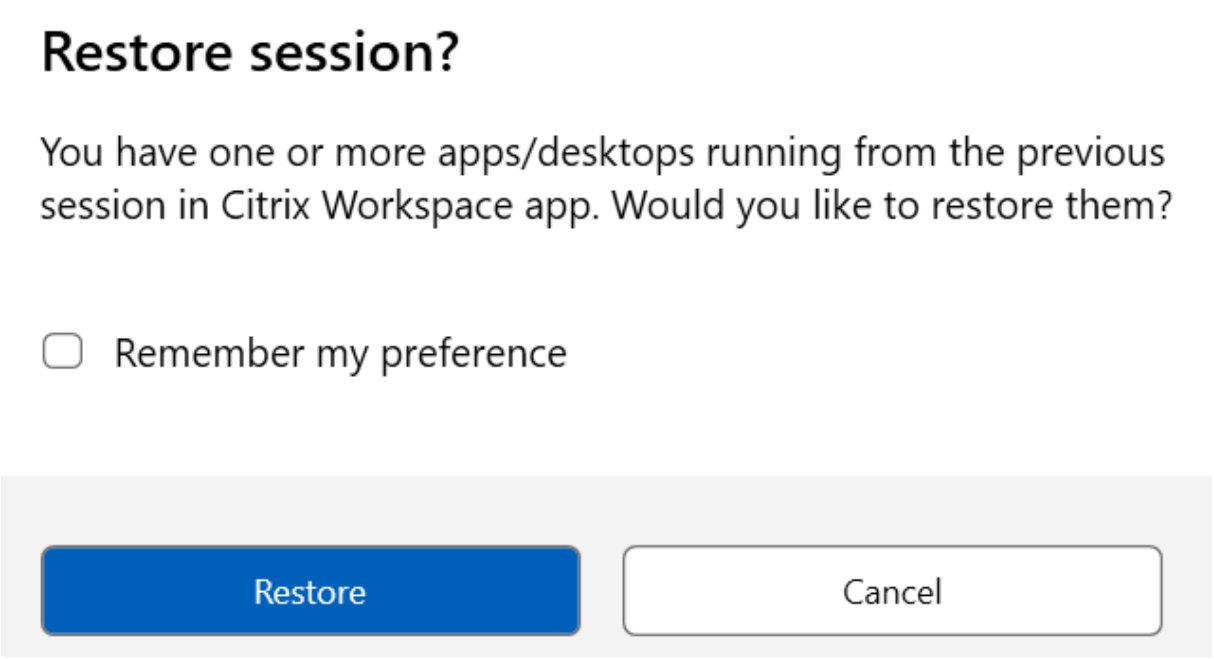
For more information, see Secure Private Access for on-premises in the Citrix Secure Private Access documentation.

2302

What's new

Improved virtual apps and desktops reconnection experience This 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:



This prompt appears only when the **show reconnection prompt to reconnect sessions** is set to true in the Global App Configuration service.

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.

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 the Configure reconnect options using Advanced Preferences dialog.

Client App Management for Zoom plug-in You can now manage the Zoom plug-in using Client App Management capability.

For more information, see Client App Management for Zoom plug-in.

Updated audio device selection behavior for optimized Microsoft Teams Starting with this release, 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.

App Protection enhancement Starting with this release, Citrix Workspace app for Windows allows you to configure App Protection for Authentication and Self-Service plug-in using the Global App Configuration. Previously, you were able to configure these components only using the Group Policy Object.

If you enable the anti-keylogging and the anti-screen capturing functionality using the Global App Configuration service, they are applicable to both Authentication and Self-Service plug-in.

> **Note:**
>
> The Global App Configuration service configurations don't apply for virtual apps, virtual desktops, web apps, and SaaS apps. These resources continue to be controlled using the Delivery Controller and Citrix Secure Private Access. For more information, see the configure section in the App Protection documentation.

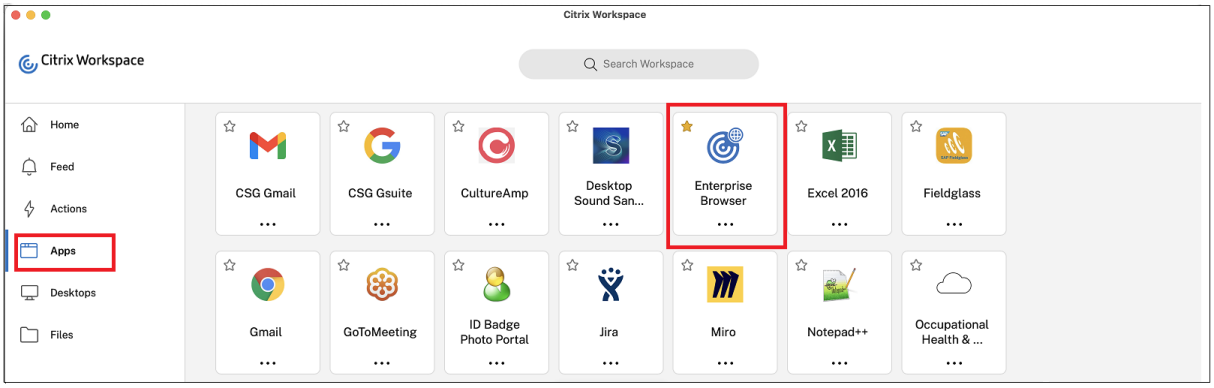
For more information, see the App Protection enhancement section.

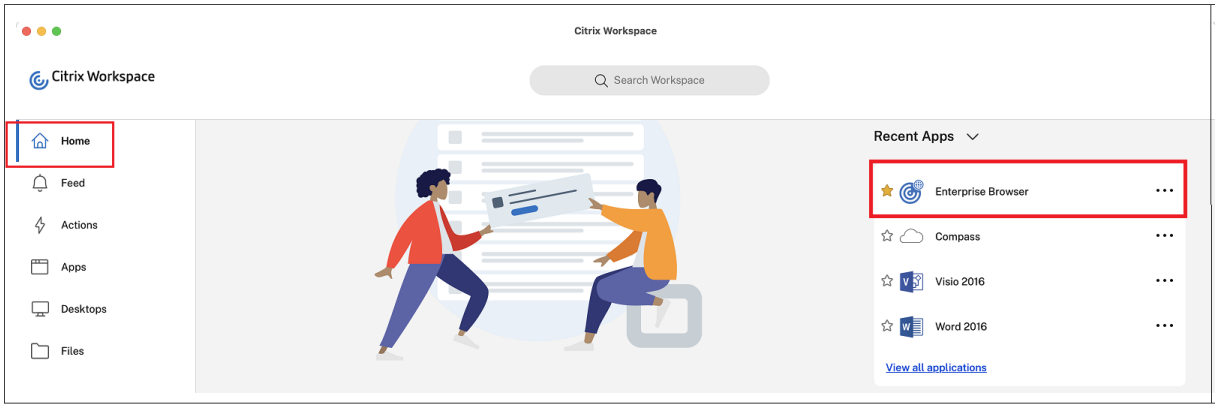
Citrix Enterprise Browser This release includes Citrix Enterprise Browser version 108.1.1.97, based on Chromium version 108. For more information about the Citrix Enterprise Browser, see the Citrix Enterprise Browser documentation.

Open all web and SaaS apps through the Citrix Enterprise Browser In this release of the Enterprise Browser (in Citrix Workspace app for Windows), all internal web apps and external SaaS apps available in the Citrix Workspace app open in Citrix Enterprise Browser.

Option to start Citrix Enterprise Browser from within Citrix Workspace app Previously, you can open the Citrix Enterprise Browser from the Citrix Workspace app after opening a web or SaaS app.

Starting with this release, you can open the Citrix Enterprise Browser from the Citrix Workspace app directly without requiring you to open a web or SaaS app. This feature provides easy access to the Citrix Enterprise Browser and doesn't require any configurations from administrators. This feature is available by default.





> **Note:**
>
> The end user must have entitlement to at least one web or SaaS app through Secure Private Access.

2212

What's new

> **Note:**
>
> From this release onward, ensure that the Microsoft Edge WebView2 Runtime version is 102 or later. For more information, see System requirements and compatibility.

Client App Management Citrix Workspace app 2212 for Windows now offers Client App Management capability that makes the Citrix Workspace app a single client app required on the end point to install and manage agents such as the Secure Access Agent and End Point Analysis (EPA) plug-in.

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

For more information, see Client App Management.

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 maximumAllowedVersion property in the Global App Config Service.

Example JSON file in Global App Config Service:

```
{

  "category": "AutoUpdate",
  "userOverride": false,
  "assignedTo": [
    "AllUsersNoAuthentication"
  ],
  "settings": [
    {

      "name": "Auto Update plugins settings",
      "value": [
        {

          "pluginSettings": {

            "upgradeToLatest": false,
            "deploymentMode": "InstallAndUpdate",
            "stream": "Current",
            "maximumAllowedVersion": "23.03.0.49",
            "minimumAllowedVersion": "0.0.0.0",
            "delayGroup": "Fast"
           }
 ,
           "pluginName": "WorkspaceApp",
           "pluginId": "1CDF566D-B2C7-47CA-802F-6283C862E1D6"
         }

       ]
     }

  ]
 }


<!--NeedCopy-->
```

When the version is set, Citrix Workspace app on the user's device is automatically updated to the version specified in the maximumAllowedVersion property.

> **Notes:**
>
> - Currently all the parameters mentioned in the preceding JSON file are mandatory. You

must provide values for the `upgradeToLatest` setting and the `maximumAllowedVersion` setting based on the requirement of your organization. However, for the remaining parameters, you can use values similar to the example JSON file.

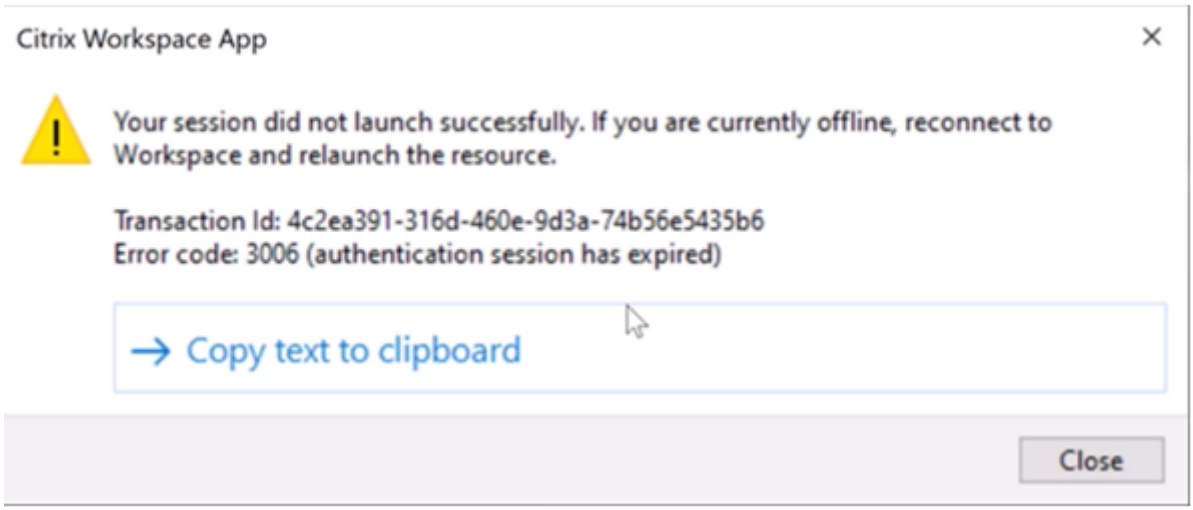
- To achieve auto-update version control, `upgradeToLatest` setting in the Global App Config Service must be set to false. If this setting is true, `maximumAllowedVersion` is ignored.
- Do not modify the pluginId as this ID is mapped to Citrix Workspace app.
- If the administrator hasn't configured the version in the Global App Config Service, Citrix Workspace app is updated to the latest available version by default.

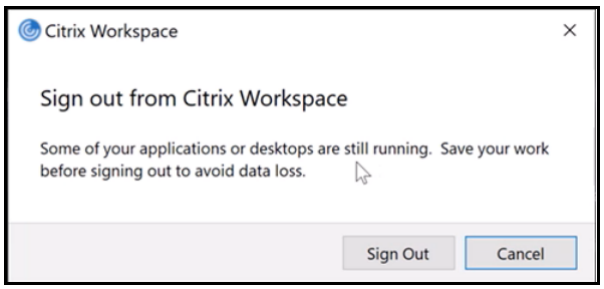
Force login prompt for Federated identity provider Citrix Workspace app now honors the Federated Identity Provider Sessions setting. For more information, see Knowledge Center article CTX253779.

You no longer need to use the Store authentication tokens policy to force the login prompt.

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 this 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**.

Support for default installation of App Protection App Protection component is now installed by default during the Citrix Workspace app installation.

The **Enable app protection** checkbox that appears during the installation is replaced with Start App Protection after installation.

When you select this checkbox, App Protection starts immediately after the installation.

> **Note:**
>
> If you do not enable this checkbox, App Protection automatically starts upon the first start of a protected resource or component for customers who have entitled to App Protection.

You can also start the App Protection component using the `/startappprotection` command line parameter. However, the previous `/includeappprotection` switch is deprecated.

> **Note:**
>
> Previously, anti-screen capture and anti-keylogging capabilities were enforced by default for Citrix authentication and Citrix Workspace app screens. However, starting from 2212, these capabilities are disabled by default and need to be configured using the Group Policy Object. For information on the GPO configuration, see Enhancement to App Protection configuration.

App Protection enhancement: Screen capture detection and notification Starting from this release, you can view a notification when a possible attempt of screen capture is made on any protected resources. For information on the resources protected by App Protection, see What does App Protection protect?

The notification appears when there is an:

- attempt to take a screenshot or record video through a screen-capturing tool.
- attempt to take a screenshot through the Print Screen key.

> **Note:**
>
> The notification appears only once per running instance of the screen capture tool. The notification appears again if you relaunch the tool and attempt screen capture.

Desktop Viewer optimization This release optimizes the Desktop Viewer experience by reducing the launch time by 5 seconds. The **Desktop Viewer** toolbar opens quickly and might display the default Windows session sign-in screen. Administrators can hide this experience by configuring the following registry to introduce some delay in milliseconds:

- Location: HKEY_CURRENT_USER\SOFTWARE\Citrix\XenDesktop\DesktopViewer
- Name: ExtendConnectScreenMS
- Type: DWORD
- Value: 00000000 (Delay in Milliseconds)

> **Note:**
>
> The registry configuration is optional.

Citrix Enterprise Browser

> **Note:**
>
> From Citrix Workspace app for Windows version 2210, the **Open all web and SaaS apps through the Citrix Enterprise Browser** feature is disabled.

This release includes Citrix Enterprise Browser version 107.1.1.13, based on Chromium version 107. For more information about the Citrix Enterprise Browser, see the Citrix Enterprise Browser documentation.

- **Set Citrix Enterprise Browser as the work browser**

  You can now configure Citrix Enterprise Browser as a work browser to open all work links. You can select an alternate browser to open non-work links.

  A work link is a link that is associated with the web or SaaS apps that are configured by the administrator for the end user. When a user clicks any link within a native application, if it's a work link, it's opened through the Enterprise Browser. If not, it's opened through the alternate browser that the end-user selects.

  For more information, see Set Citrix Enterprise Browser as the work browser.

2210.5

What's new

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

Enhancement to auto-update Citrix Workspace app now supports auto-update when Proxy auto-configuration (PAC) and Web Proxy Auto-Discovery Protocol (WPAD) detection is enabled.

Citrix Enterprise Browser This release includes Citrix Enterprise Browser version 105.2.1.40, based on Chromium version 105. For more information about the Citrix Enterprise Browser, see the Citrix Enterprise Browser documentation.

2210

What's new

Background blurring for webcam redirection Citrix Workspace app for Windows now supports background blurring for webcam redirection. You can enable this feature by selecting the **Preferences** > **Connections** > **Enable background blur** checkbox.

App Protection enhancements for web and SaaS apps on Windows 11 This App Protection enhancement optimizes the experience and security capabilities for web and SaaS app users on Windows 11. This enhancement is available via the Citrix Enterprise Browser for Secure Private Access customers.

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\HDX

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.

Citrix Enterprise Browser This release includes Citrix Enterprise Browser version 105.1.1.27, based on Chromium version 105. For more information about the Citrix Enterprise Browser, see the Citrix

Enterprise Browser documentation.

Rebranding Citrix Workspace Browser Citrix Workspace Browser is now Citrix Enterprise Browser. The custom scheme is now changed from citrixworkspace:// to citrixbrowser://.

Implementing this transition in our products and their documentation is an ongoing process. Your patience during this transition is appreciated.

- The product UI, in-product content, and the images and instructions in the product documentation will be updated in the coming weeks.
- It is possible that some items (such as commands and MSIs) might continue to retain their former names to prevent breaking existing customer scripts.
- Related product documentation and other resources (such as videos and blog posts) that are linked from this product documentation might still contain former names.

Open all web and SaaS apps through the Citrix Enterprise Browser From this release, all internal web apps and external SaaS apps available in the Citrix Workspace app open in Citrix Enterprise Browser.

> **Note:**
>
> From Citrix Workspace app for Windows version 2210, the **Open all web and SaaS apps through the Citrix Enterprise Browser** feature is disabled.

Supporting auto-update of Citrix Workspace app on VDA You can now enable the auto-update feature on VDA by creating the following registry value:

On a 32-bit machine:

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

On a 64-bit machine:

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

Citrix Enterprise Browser (formerly Citrix Workspace Browser) This release includes Citrix Enterprise Browser version 103.2.1.10, based on Chromium version 103. For more information about the Citrix Enterprise Browser, see the Citrix Enterprise Browser documentation.

- **Citrix Enterprise Browser Profiles**

  Profiles help you keep personal information such as history, bookmarks, passwords, and other settings separate for each of your Citrix Workspace accounts. Based on your Workspace store, a profile is created, allowing you to have a unique and personalized browsing experience.

  > **Note:**
  >
  > After you upgrade to version 103.2.1.10 and sign in to the device for the first time, only your previously saved passwords are removed. When you sign in to the device using a different store for the first time, all your previously saved data is lost.

2207

What's new

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.

> **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:

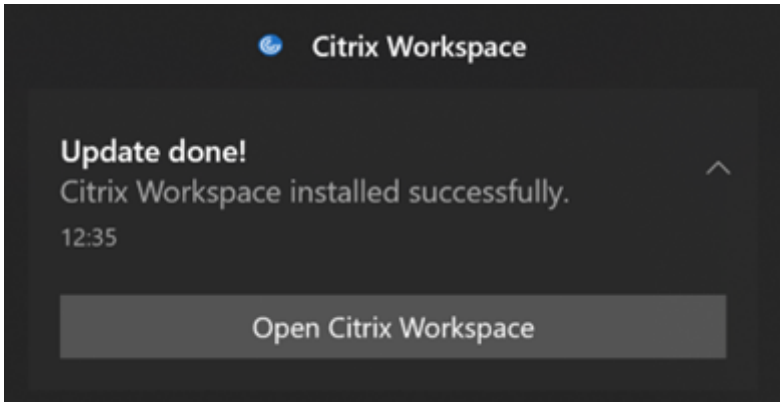
- Admin and user-defined background replacement isn't supported.
- The background effect doesn't persist between sessions. When you close and relaunch Microsoft Teams or VDA is reconnected, the background effect is reset to off.
- After the ICA session is reconnected, the effect is off. However, the 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 the future update roll-out from Microsoft Teams. When the update is rolled-out by Microsoft, you can check Knowledge Center articleCTX253754 and the Microsoft 365 Public roadmap for the documentation update and the announcement.

Improved auto-update experience The auto-update feature automatically updates the Citrix Workspace app to the latest version without the need for any user intervention.

Citrix Workspace app periodically checks and downloads the latest available version of the app. Citrix Workspace app determines the best time to install based on user activity not to cause any disruptions.

When the installation is complete, the following notification appears:



If the Citrix Workspace app can't find the right time to install the updates in the background, a notification prompt appears.

Citrix Enterprise Browser This release includes Citrix Enterprise Browser version 102.1.1.14, based on Chromium version 102.

Note on Citrix Workspace app update While updating Citrix Workspace app for Windows from the previous version to 2207, the user is prompted to sign in. The sign-in is prompted only for the workspace store.

2206

What's new

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.

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. For more information, see Knowledge Center article CTX460068.

Citrix Enterprise Browser This release includes Citrix Enterprise Browser version 101.1.1.12, based on Chromium version 101. For features or bugs fixes in the Citrix Enterprise Browser, see What's new in the Citrix Enterprise Browser documentation.

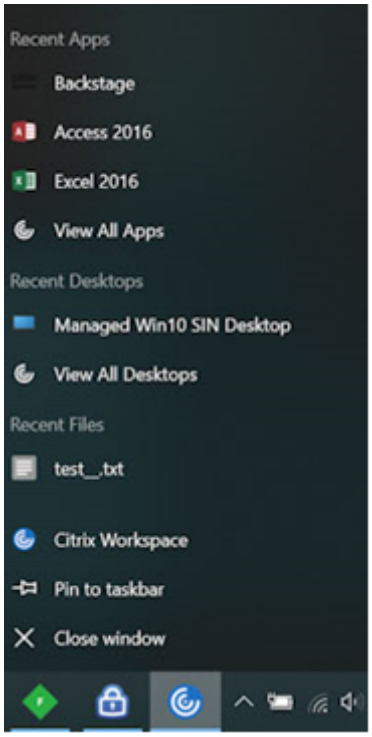
2205

What's new

> **Note:**
>
> From this release onward, ensure that the Microsoft Edge WebView2 Runtime version is 99 or later. For more information, see System requirements and compatibility.

Change to Citrix Casting Previously, Citrix Casting was enabled by default during the Citrix Workspace app installation. Starting from this 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.

Quick access to resources Starting from this 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.



Sign out custom web store upon Citrix Workspace app exit When the `signoutCustomWebstoreOnExit` attribute is set to True, closing the Citrix Workspace app signs you out of custom webstores. You can configure the `signoutCustomWebstoreOnExit` attribute in **Global App Configuration Service**.

For more information, see Global App Configuration Service documentation.

Support to open Citrix Workspace app in maximized mode Starting from this 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.

Storebrowse support for Workspace Citrix Workspace app for Windows now provides Storebrowse support to self-service that enables Storebrowse users to access Cloud and Workspace features.

> **Note:**
>
> - 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.

For more information, see Storebrowse for Workspace.

Citrix Enterprise Browser

- This release includes Citrix Enterprise Browser version 99.1.1.8, based on Chromium version 99. For features or bugs fixes in the Citrix Enterprise Browser, see What's new in the Citrix Enterprise Browser documentation.
- Citrix Workspace app now alerts you about closing active browser windows, when you do any of the following in the Citrix Workspace app:
  - Sign out from a store
  - Switch to a different store
  - Add a new store
  - Delete the current store

2204.1

What's new

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

Citrix Enterprise Browser This release includes Citrix Enterprise Browser version 98.1.2.20, based on Chromium version 98. For features or bugs fixes in the Citrix Enterprise Browser, see What's new in the Citrix Enterprise Browser documentation.

Microsoft Teams optimization

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

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

February 14, 2024

Fixed issues in 2402 LTSR

- You might notice that there's no automatic focus inside the virtual desktop that is opened in full-screen mode. You must click inside the session to regain focus. [RFWIN-32051]
- On reconnecting published apps an extra instance of a published app gets opened. [CVADHELP-24485]
- The Windows Surface touch pad and soft keyboard might not be supported on the Citrix Workspace app sign-in screen. This issue occurs when you sign in to a session that is published from Windows VDA in full-screen mode. As as a workaround, open the session in window mode and then sign in to the Citrix Workspace app. [RFWIN-32050]
- Two instances of a published application, for example app1, are observed after app1 is disconnected and another app is launched from the same VDA. [RFWIN-32517]
- The version of the Chromium Embedded Framework (CEF) is upgraded to 120. This version upgrade helps to resolve security vulnerabilities.
- For Citrix Workspace app 2402 LTSR version, the BCR client components aren't installed or upgraded by default with the CWA Installer UI. For new installation or upgrades, you can install the BCR Client components with other required components via the ADDLOCAL command line parameter. For more information, see Install one or more of the specific components.
  If the Citrix Workspace app installer UI was used, you can install the BCR Client components post installation using the `BCR_Client.msi` from the `%ProgramFiles(x86)%\Citrix\Citrix Workspace 2402` directory. [HDX-60108] [HDX-61734]

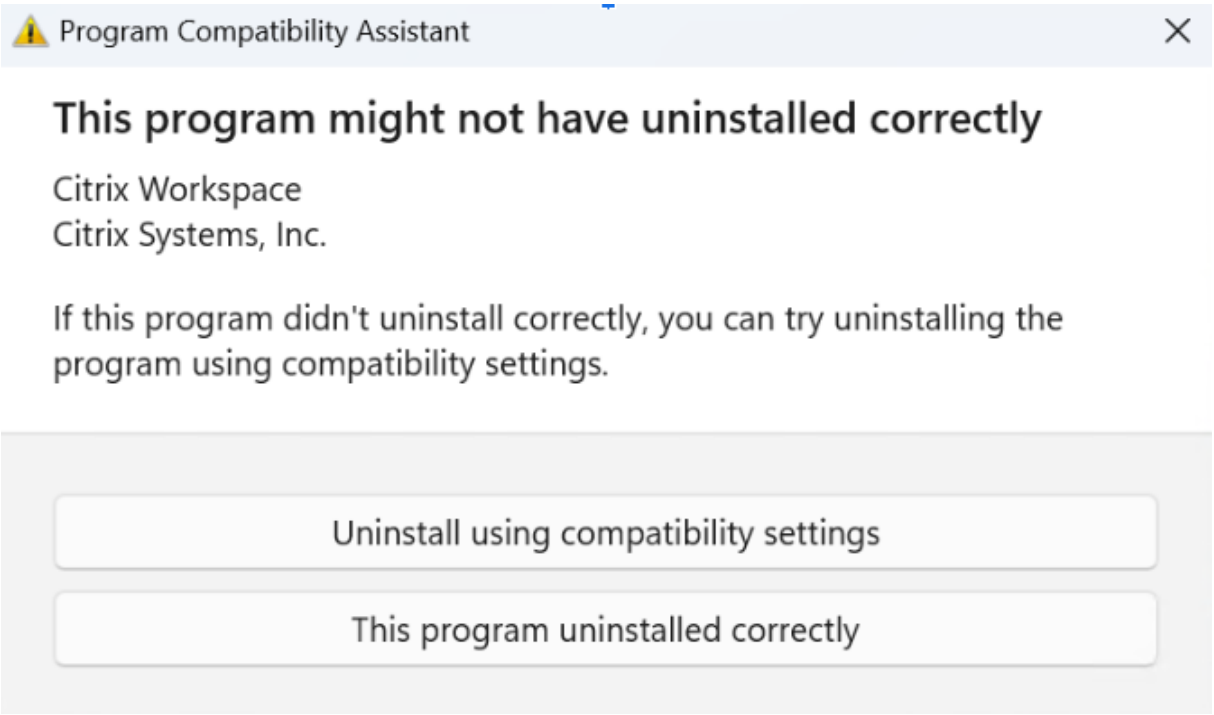
- For `Windows 10 32bits x86` version, the **Enable Background blur** checkbox is removed as the background blur effect isn't supported on this version. [HDX-60308]
- You might notice visual artifacts when attempting to split the screen or adjust the primary monitor within the **Monitor Layout** tab on the **Preferences** screen. [HDX-59798]
- Windows Media Player (WMP) shows a black screen with rave enabled on one monitor when the primary monitor isn't the leftmost monitor (when multiple GPUs are involved). To resolve this issue the default renderer has been changed from **VMR9** to **EVR**.
  If you want to disable **EVR**, create DWORD AllowEvrH264 = 0 under `Computer\HKEY_CURRENT_USER\Software\Citrix\HDXMediaStream`. [HDX-60494]
- When you share screen including the computer sound, if multiple audio output devices are playing sound, one or more receivers might notice sound artifacts. [HDX-48213]
- BCR might play multiple audio streams at the same time instead of one active stream. [HDX-61600]
- If you use external monitors and then switch to a single monitor (for example laptop), the size of Citrix Workspace app menu options, UI text, and dialog boxes might appear smaller than the normal display size. [HDX-47575]
- If you're using mono audio for stereo audio streams, you might hear only one audio channel in one earpiece instead of receiving both channels on both ears. [HDX-56344]

Known issues

February 14, 2024

Known issues in 2402 LTSR

While uninstalling Citrix Workspace app 2402 LTSR for Windows - Preview version from the **Control Panel** > **Programs** > **Programs and Features**, the following pop-up appears:



The issue occurs intermittently on Windows 11 machines. Also, this issue doesn't occur in any other uninstallation methods including uninstall from **Start** > **Apps** > **Apps & Features**. The uninstallation is completed successfully even though you get the preceding error message. You can click **This program uninstalled correctly** or click the "X"button on the top to ignore the warning message. [RFWIN-32669]

System requirements and compatibility

February 14, 2024

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 does not appear but the error message is recorded in the `\Citrix\Logs\CTXWorkspaceInstallLogs-*`.

Software requirements

- Microsoft Edge WebView2 Runtime version 119 or later
- .NET Framework 4.8 and .NET Desktop Runtime 6.0.25 or later
- Latest version of Microsoft Visual C++ Redistributable

> **Note:**
>
> To handle any security patches from Microsoft or other third party dependent components (eg: .NET Core, .NET Framework, VC redistributable, Edge webview), you can use one of the following methods:
>
> ```
> 1 - Enable Windows auto update on client machines
> 2 - 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 internet. Alternatively, you can install the suitable offline Microsoft Edge WebView2 Runtime Evergreen Standalone Installer package before installing Citrix Workspace app.
- The device must have access to the following URLs:

- `https://*.dl.delivery.mp.microsoft.com` to download Microsoft Edge WebView2 Runtime during the Citrix Workspace app installation. For more information, see Allow list for Microsoft Edge endpoints.
- `https://msedge.api.cdp.microsoft.com` to check for Microsoft Edge WebView2 Runtime update
- Internet connection
- The device must have access to the following URLs:

> **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 x86 version of.NET Desktop Runtime 6.0.25 or later. You must install the x86 version even on x64 system.
- In case of 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 with non-administrator privileges and .NET Framework 4.8 and .NET Desktop Runtime 6.0.25 or later aren't 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 2309 or later requires the x86 version of.NET Desktop Runtime 6.0.25 or later for both x86 and x64 systems.	Method 1: Citrix Workspace app installs .NET Framework 4.8 and the latest version of.NET Desktop Runtime 6.0 along with the app installation. This installation is an online install and requires internet connectivity. The device must have access to the `downloadplugins.citrix.com` domain URL. 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 requirements using a deployment method, for example, SCCM. Method 3: Admins can install .NET Framework 4.8 and .NET Desktop Runtime 6.0.25 from the Microsoft site separately before installing Citrix Workspace app. It is recommended to download the latest version of .NET Desktop Runtime 6.0 (6.0.25 or later).

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

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

Starting with Version 1904, 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.

For troubleshooting issues with the .NET Framework or the Microsoft Visual C++ Redistributable installation, see Citrix Knowledge Center article CTX250044.

Connectivity requirements

Feature flag management If an issue occurs with Citrix Workspace app in production, use feature flags and a third-party service called LaunchDarkly to disable an affected feature dynamically in Citrix Workspace app even after the feature is shipped.

You do not need to make any configurations to enable traffic to LaunchDarkly, except when you have a firewall or proxy blocking outbound traffic. In that case, you enable traffic to LaunchDarkly via specific URLs or IP addresses, depending on your policy requirements.

You can enable traffic to the following URLs:

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

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

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

- LaunchDarkly service
- APNs listener service

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

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

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
Windows 10 Enterprise (32-bit and 64-bit Editions). For more information about compatible Windows 10 versions, see Windows 10 Compatibility with Citrix Workspace app for Windows.
Windows 10 Enterprise (2016 LTSB 1607, LTSC 2019)
Windows 10 (Home edition*, Pro)
Windows Server 2022
Windows Server 2019
Windows Server 2016

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

Windows 10 or 11 Compatibility with Citrix Workspace app for Windows

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
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.

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

Windows 11 Version number	Build number	Citrix Workspace app Version
23H2	22631	2311 and later
22H2	22621	2209 and later
21H2	22000	2109.1 and later

Install and uninstall

February 2, 2024

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 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.

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 Citrix Ready workspace hub with Citrix Workspace app for Windows..

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

	Installation folder	Installation type
Administrator	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:

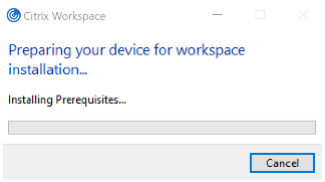
```
CitrixWorkspaceApp.exe /CleanInstall
<!--NeedCopy-->
```

User interface based installation

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

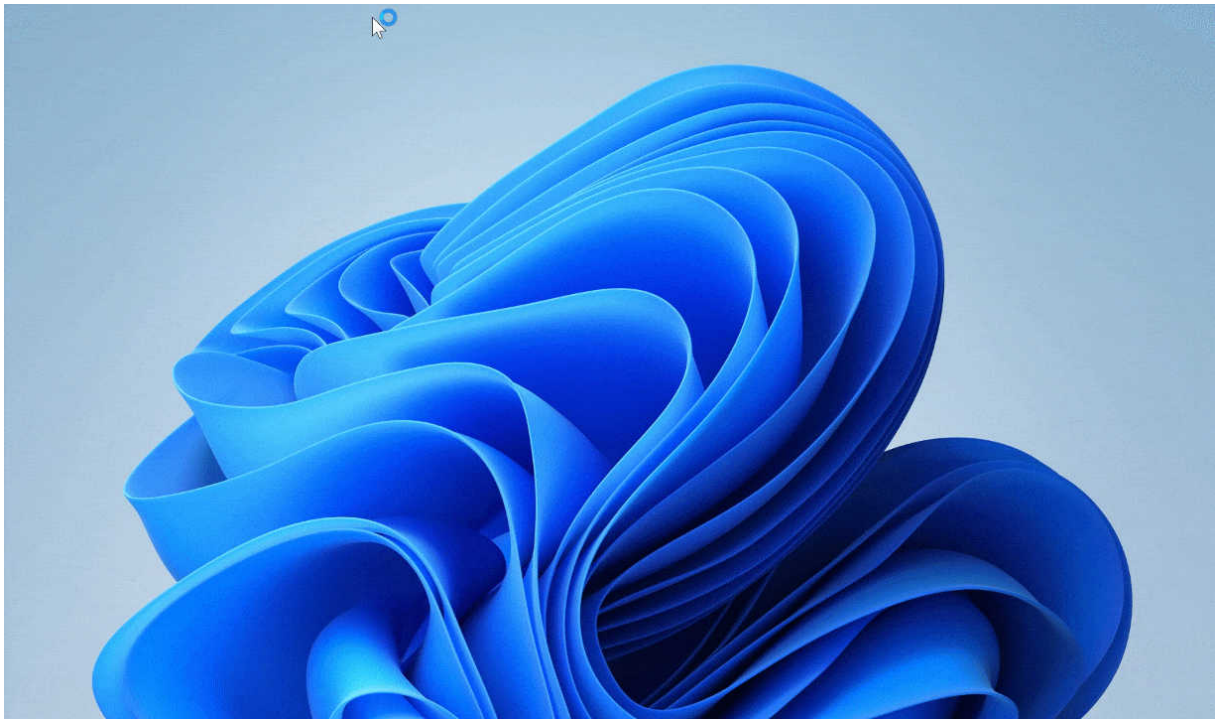
1. Launch the `CitrixWorkspaceApp.exe` file.

   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, if required to enable the App Protection feature select the **Start App Protection after installation** checkbox. Citrix Workspace app installation continues and successfully completes.

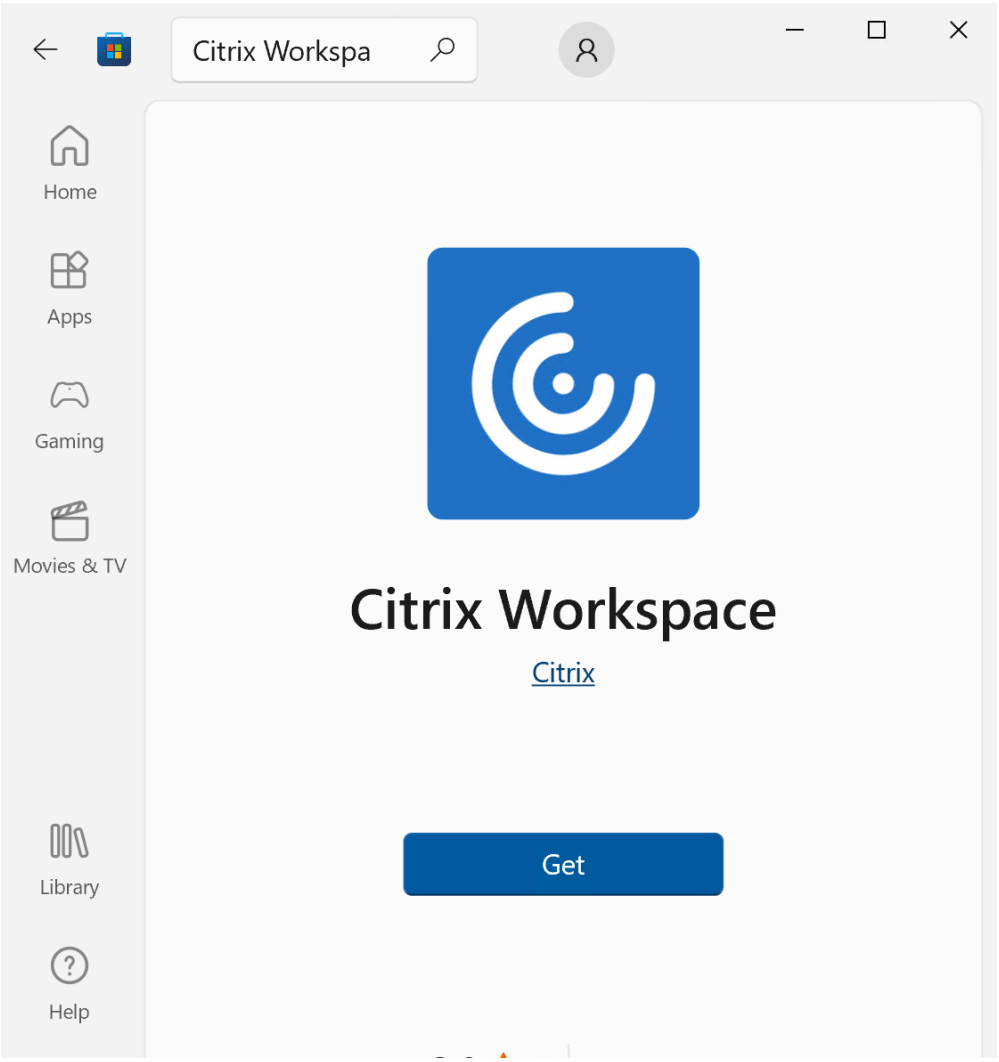


Important:

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.
`noreboot`	Suppresses the prompts to reboot during installation. When you suppress the reboot prompt, USB devices that are in a suspended state aren't recognized. The USB devices are activated only after the device is restarted.
`/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.

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`.

AutoUpdateStream command value	Description	Example
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 later** option is displayed in the 'n'count.	`CitrixWorkspaceApp.exe DeferUpdateCount=<n>`

> **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`

ALLOWADDSTORE command value	Description	Example
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`
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:

```
1 CitrixWorkspaceApp.exe /silent
2 STORE0="AppStore;https://testserver.net/Citrix/MyStore/discovery;on;HR
     App Store
3
4 <!--NeedCopy-->
```

To specify the Citrix Gateway store URL:


```
CitrixWorkspaceApp.exe  STORE0= HRStore;https://ag.mycompany.com#
    Storename;On;Store
<!--NeedCopy-->
```

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

> **Note:**
>
> - In a multi-store setup, only one Citrix Gateway store URL configuration is allowed and that must be first in the list (parameter STORE0).
> - 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= NetScaler Store;https://ag.mycompany.
    com#Storename;On;NetScaler Store
STORE1="StoreFront Store;https://testserver.net/Citrix/MyBackupStore/
    discovery;on; StoreFrontStore
<!--NeedCopy-->
```

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

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 App Protection.

> **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: `InstallEmbeddedBrowser`
- Description: Excludes the Citrix Enterprise Browser binaries.
- Example: Run the `InstallEmbeddedBrowser=N` switch to exclude the embedded browser feature.

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 Browserbinaries.

If your version of Citrix Workspace app includes the Citrix Enterprise Browser binaries and you are upgrading to Version 2002, the Citrix Enterprise Browser binaries are automatically updated during the upgrade.

Specify custom installation directory

- Command: `INSTALLDIR`
- Description: Specifies the custom installation directory for 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:**
>
> 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 browse 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	ingle 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.
WorkspaceHub	Win Docker	Provides a way to expand a user's workspace, making mirroring or extending local display wirelessly.
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,SelfService,WebHelper,WorkspaceHub,
    CitrixEnterpriseBrowser
<!--NeedCopy-->
```


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

Install Citrix Casting

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

For more information on Citrix Casting, see Citrix Casting.

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`
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 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.	`CitrixWorkspaceApp.exe LEGACYFTAICONS=False`
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 value for the `CLIENT_NAME` property.	`CitrixWorkspaceApp.exe ENABLE_DYNAMIC_CLIENT_NAME=No`

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`

> **Note:**
>
> 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
<!--NeedCopy-->
```

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

```
CitrixWorkspaceApp.exe /silent /uninstall
<!--NeedCopy-->
```

> **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`.

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

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
<!--NeedCopy-->
```

For silent reset, use the following command:

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


> **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

October 7, 2023

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

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

Using Active Directory and sample scripts

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

To use the scripts with Active Directory:

1. Create the Organizational Unit (OU) for each script.

2. Create a Group Policy Object (GPO) for the newly created OU.

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	`CheckAndDeployWorkspacePerMachine.bat`	`CheckAndRemoveWorkspacePerMachine.bat`
Per-user	`CheckAndDeployWorkspacePerUserLogon.bat`	`CheckAndRemoveWorkspacePerUserLogon.bat`

To add the startup scripts:

1. Open the Group Policy Management Console.
2. Select **Computer Configuration** or **User Configuration** > **Policies** > **Windows Settings** > **Scripts**.

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

To deploy Citrix Workspace app for Windows:

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

To remove Citrix Workspace app for Windows:

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

Using workspace for web

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

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

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

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

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

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

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

Using System Center Configuration Manager 2012 R2

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

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

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

Adding Citrix Workspace app to the SCCM deployment

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

> tem 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

November 16, 2023

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 pre-configured 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: Workspace, StoreFront, Citrix Gateway Store, and Custom web store.

Workspace

Citrix Workspace is a cloud-based enterprise app store that provides secure and unified access to apps, desktops, and content (resources) from anywhere, on any device. These resources can be Citrix DaaS, content apps, local and mobile apps, SaaS and Web apps, and browser apps. For more information, see Citrix Workspace Overview.

StoreFront

StoreFront is an on-premises enterprise app store that aggregates applications and desktops from Citrix Virtual Apps and Desktops sites into a single easy-to-use store for users.

For more information, see StoreFront documentation.

Citrix Gateway Store

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

Custom web stores

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

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

You can 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**.

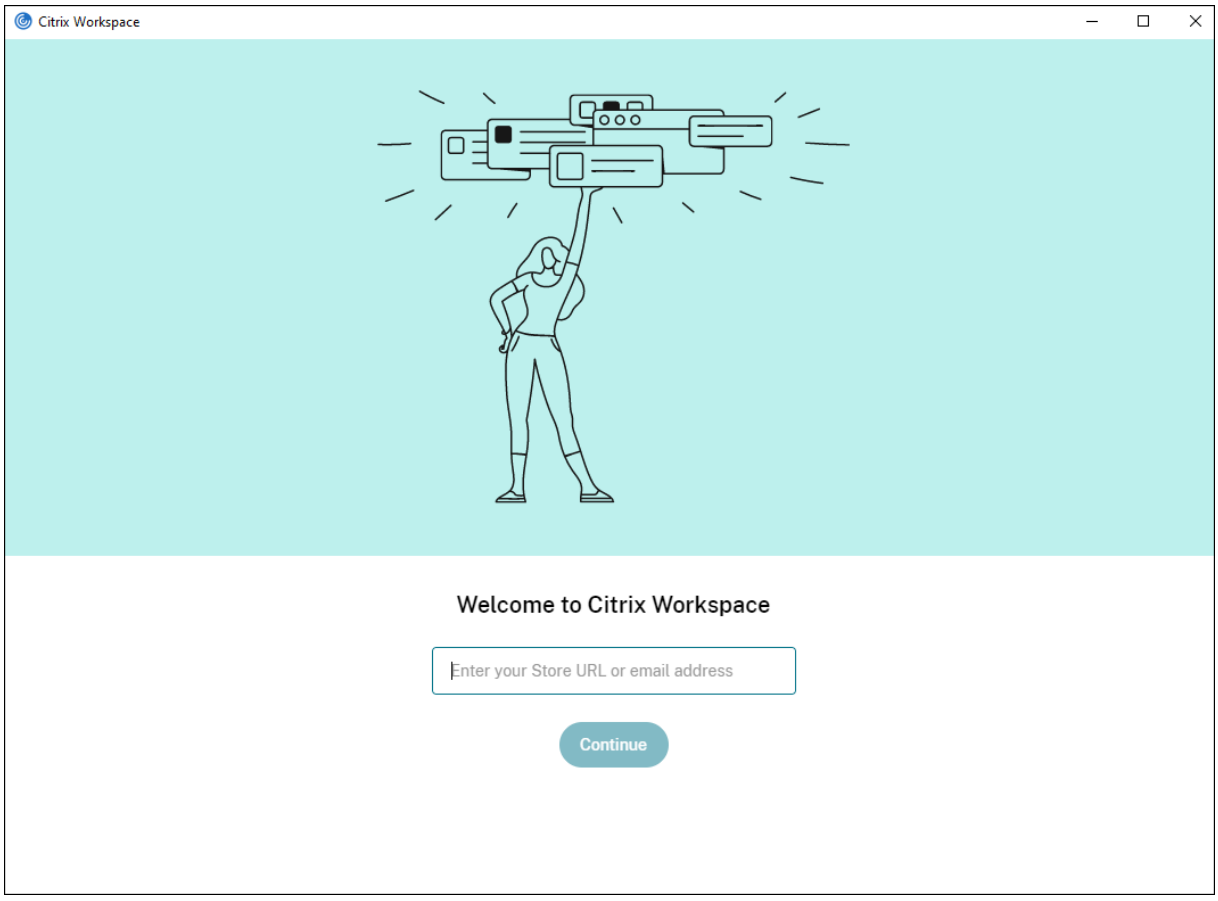
Adding store URL to Citrix Workspace app

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

- 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 log on to the account.



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

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

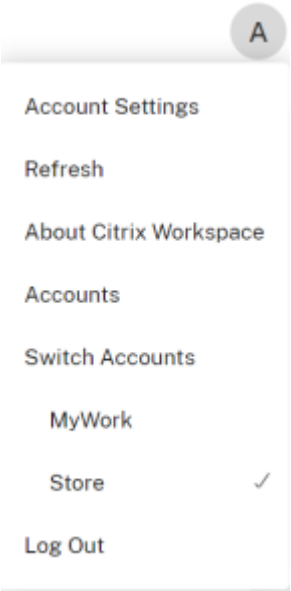
    CitrixGatewayFQDN?MyStoreName:

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

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

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

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



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 Man-**

ager. 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 determines the Citrix Gateway or StoreFront Server associated with the email address based on Domain Name System (DNS) Service (SRV) records. The app then prompts the user to log on to access virtual desktops and applications.

To configure email-based account discovery for Citrix Workspace stores, see Getting started in the Global App Configuration Service documentation.
To configure email-based account discovery for Citrix StoreFront or Citrix Gateway stores, see Configuring email-based account discovery.

Adding store through CLI

Install Citrix Workspace app for Windows as an administrator using the command-line interface.

For more information, see List of command-line parameters.

Provide users with provisioning files

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

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

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

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 **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]://servername.domain/IISLocation/discovery
   ;[On, Off]; [storedescription]"
   ```

   Values:

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

7. Add or specify the Citrix Gateway URL. Enter the name of the URL, delimited by a semi-colon:

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

   Where #Store name is the name of the store behind Citrix Gateway.

> **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.
> - 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.

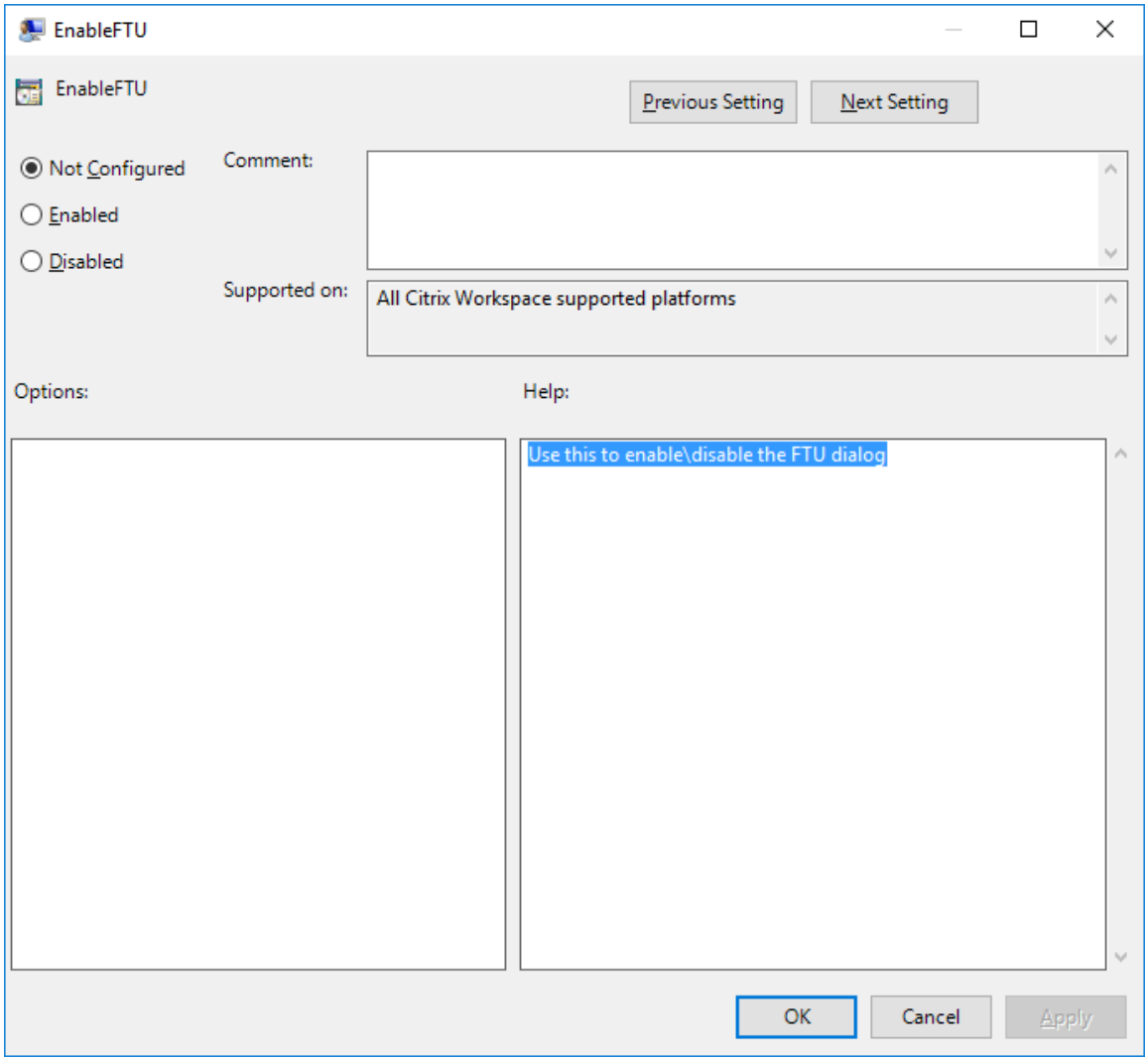
Starting with Version 1808, changes made to the Citrix Gateway URL/StoreFront Account List policy are applied in a session after app restart. A reset isn't required.

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

Limitations:

- Citrix Gateway URL must be listed first followed by StoreFront URLs.
- No support for Multiple Citrix Gateway URLs.

> **Note:**
>
> Users can also access the store via a web browser. Users can log in to the Citrix Store from a web browser and launch a virtual app or desktop from the web. The virtual app or desktop launch leverages the capabilities of the natively installed Citrix Workspace app.
>
> In this case, it may be desirable to hide the **Add Account** prompt from users. This can be achieved via the following setting:
>
> - **Renaming Citrix execution file**: Rename the **CitrixWorkspaceApp.exe** to **CitrixWorkspaceAppWeb.exe** to alter the behavior of **Add Account** dialog. When you rename the file, the **Add Account** dialog is not displayed from the **Start** menu.
> - **Group Policy Object administrative template**: To hide the **Add Account** option from the Citrix Workspace app installation wizard, disable **EnableFTUpolicy** under Self-Service node in Local Group Policy Object administrative template as shown below. This is a per-machine setting, hence the behavior is applicable for all users.



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.

Connect

Citrix Workspace app provides users with secure, self-service access to virtual desktops and applications, and on-demand access to Windows, web, and Software as a Service (SaaS) applications. Citrix StoreFront or legacy webpages created with Web Interface manage the user access.

To connect to resources using the Citrix Workspace UI

The Citrix Workspace app home page displays virtual desktops and applications that are available to the users based on their account settings (that is, the server they connect to) and settings configured by Citrix Virtual Apps and Desktops or Citrix DaaS administrators. Using the **Preferences** > **Accounts** page, you can configure the URL of a StoreFront server or, if email-based account discovery is configured, by entering the email address.

After connecting to a store, the self-service shows the tabs: **Favorites**, **Desktops**, and **Apps**. To launch a session, click the appropriate icon. To add an icon to **Favorites**, click the **…** icon and select **Add to favorites**.

StoreFront to Workspace URL Migration

StoreFront to Workspace URL migration enables you to seamlessly migrate your end users from a StoreFront store to Workspace store with minimal user interaction.

Consider, all your end users have a StoreFront store `storefront.com` added to their Citrix Workspace app. As an administrator, you can configure a StoreFront URL to Workspace URL Mapping {

‘storefront.com’:’xyz.cloud.com’} in the Global App Configuration Service. The Global App Config Service pushes the setting to all Citrix Workspace app instances, on both managed and unmanaged devices, that have the StoreFront URL `storefront.com` added.

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

To enable the feature, do the following steps:

1. Configure StoreFront to Workspace mapping using the Global App Config Service. For more information on Global App config service, 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
         }

       ]
       }

     ]
     }

   }

  }


<!--NeedCopy-->
```

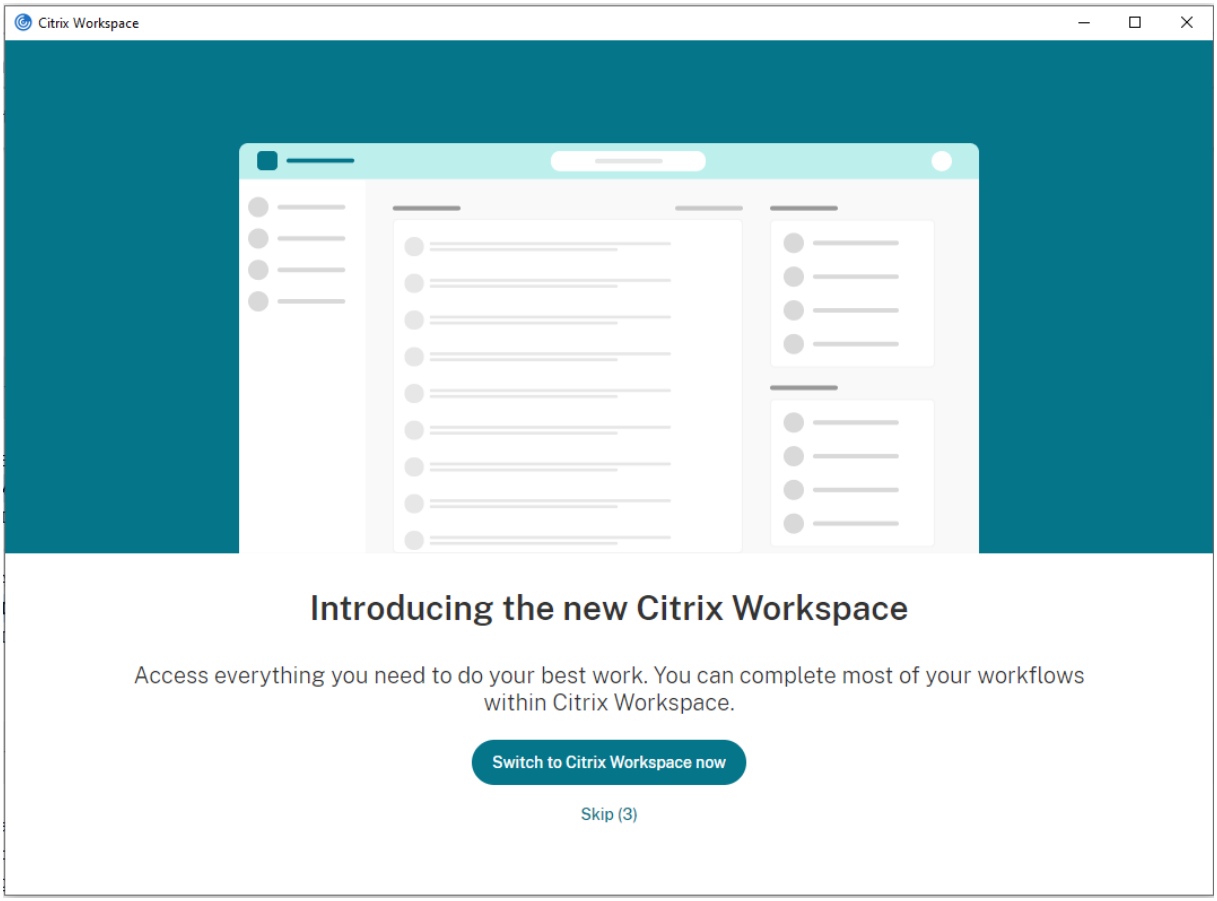
> **Note:**
>
> If you're configuring the payload for the first time, use POST.
> If you're editing the existing payload configuration, use PUT and check that you have the payload that consists of all the supported settings.

3. Specify the StoreFront URL `storefront.com` as the value for **URL** in the **serviceURL** section.
4. Configure the Workspace 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 Workspace 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 2112.1 release, admins can configure the discovery and enumeration of locally installed applications within the Citrix Workspace app. You can configure this feature by using the Global App Configuration Service. For more information about configuring this feature, 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.

Updates and plugins management

September 26, 2023

This section describes the following:

- Updates
- Plugins management

Update

November 30, 2023

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\CitrixOnlinePluginPackWeb` location.

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

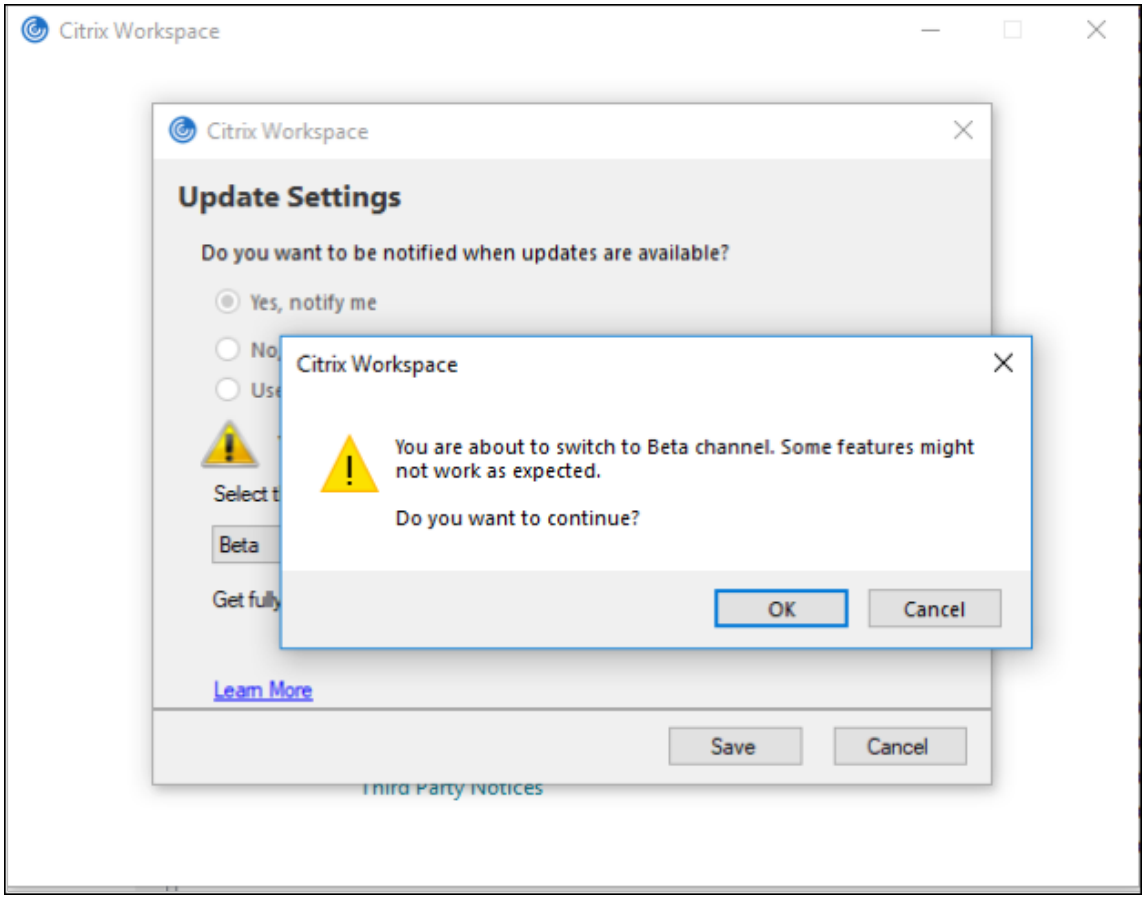
1. Right-click Citrix Workspace app icon from the notification area.
2. Select **Advanced Preferences**.

   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 maximumAllowedVersion property in the Global App Config Service.

Example JSON file in Global App Config Service:

```
{

  "category": "AutoUpdate",
  "userOverride": false,
  "assignedTo": [
    "AllUsersNoAuthentication"
  ],
  "settings": [
```



```
    {

      "name": "Auto Update plugins settings",
      "value": [
        {

          "pluginSettings": {

            "upgradeToLatest": false,
            "deploymentMode": "InstallAndUpdate",
            "stream": "Current",
            "maximumAllowedVersion": "23.03.0.49",
            "minimumAllowedVersion": "0.0.0.0",
            "delayGroup": "Fast"
          }
,
          "pluginName": "WorkspaceApp",
          "pluginId": "1CDF566D-B2C7-47CA-802F-6283C862E1D6"
        }

      ]
    }

  ]
 }


<!--NeedCopy-->
```

When the version is set, Citrix Workspace app on the user's device is automatically updated to the version specified in the maximumAllowedVersion property.

> **Notes:**
>
> - Currently all the parameters mentioned in the preceding JSON file are mandatory. You must provide values for `upgradeToLatest` setting and the `maximumAllowedVersion` setting based on the requirement of your organization. However, for the remaining parameters, you can use values similiar to the example JSON file.
> - To achieve auto-update version control, `upgradeToLatest` setting in the Global App Config Service must be set to false. If this is true, `maximumAllowedVersion` will be ignored.
> - Do not modify the pluginId as this is mapped to Citrix Workspace app.
> - 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.

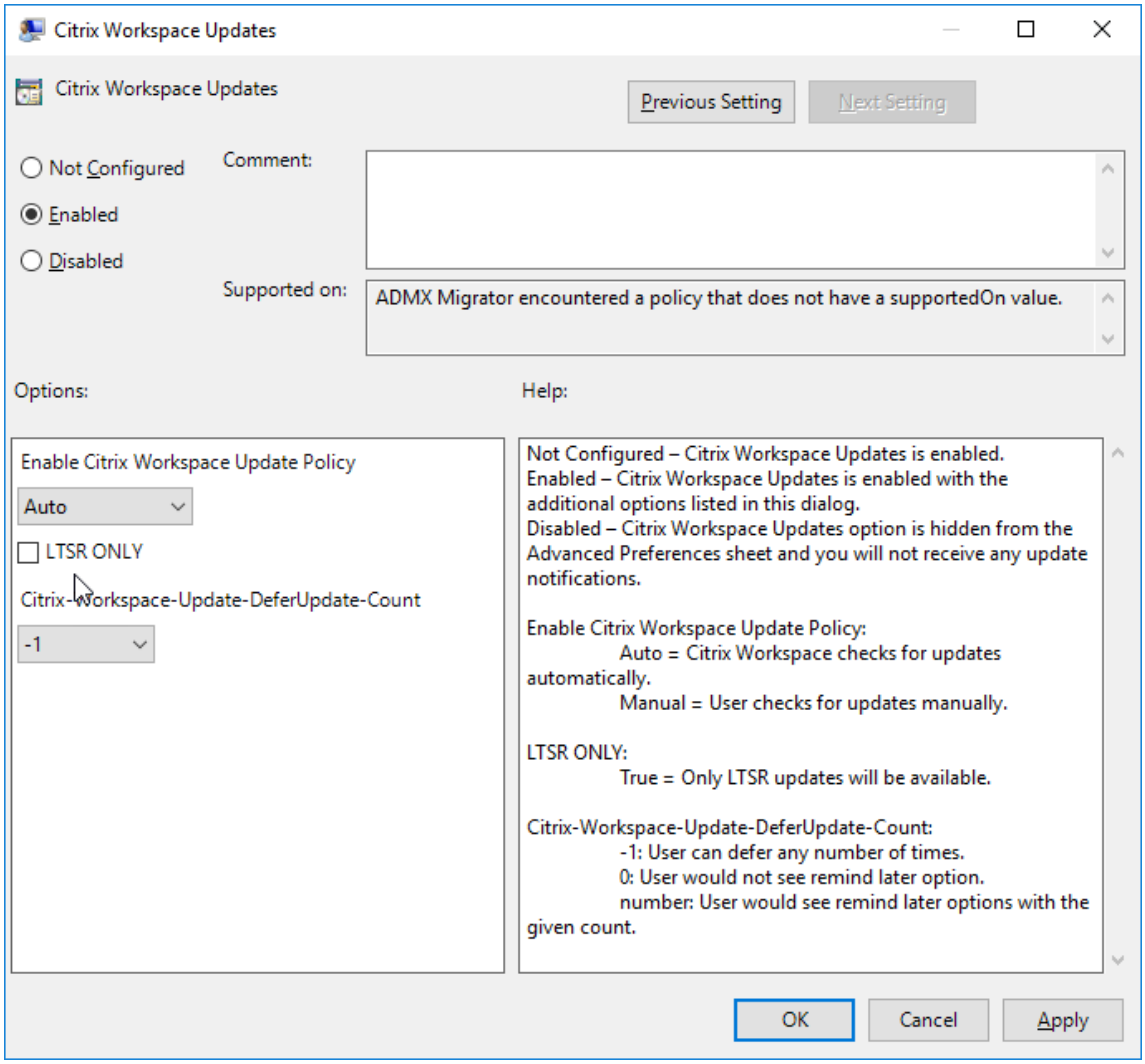
Advanced configuration for automatic updates (Citrix Workspace Updates)

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.

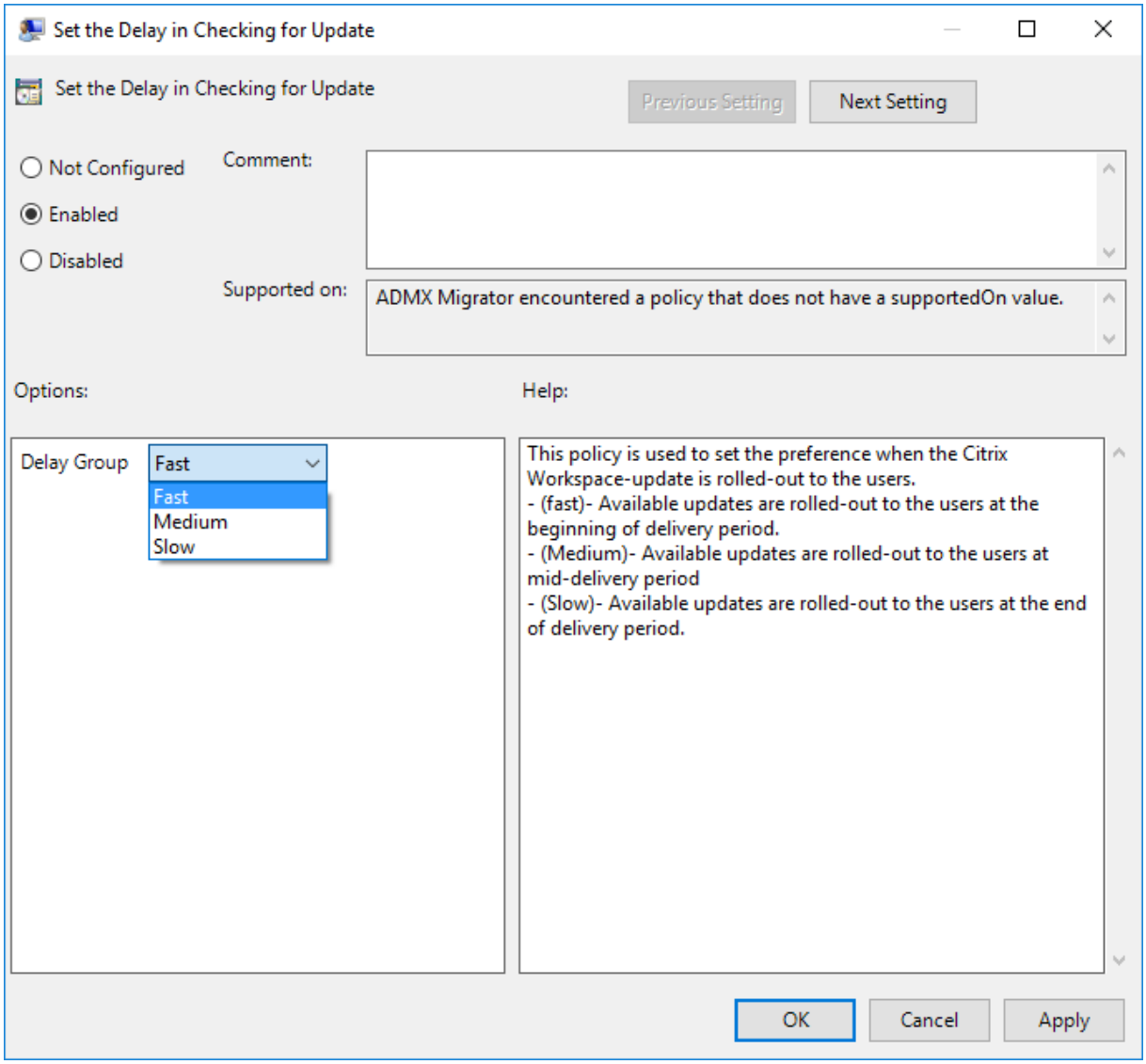
> **Note:**
>
> When you select **Disabled**, you aren't notified of new updates. **Disabled** option also hides the Workspace Updates option from the Advanced Preferences sheet.

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,

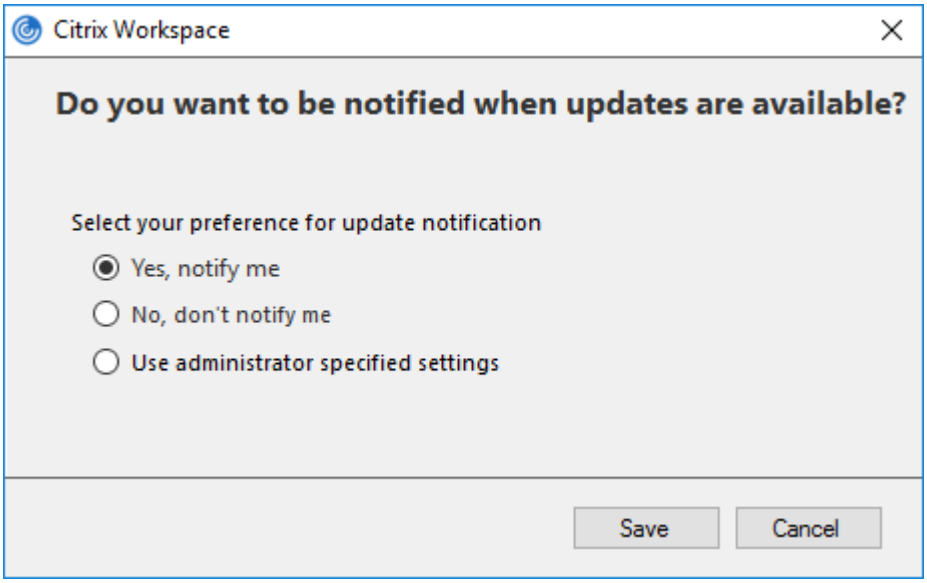
```
CitrixReceiverUpdater.exe /AutoUpdateCheck=auto /AutoUpdateStream=
Current /DeferUpdateCount=-1 /AURolloutPriority=fast
```

> **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>
 <!--NeedCopy-->
```

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>

```



```
51            <clear />
52
53          </plugins>
54
55          <trustSettings>
56
57            <clear />
58
59          </trustSettings>
60
61          <properties>
62
63            <clear />
64
65          </properties>
66
67        </metadata>
68
69      </account>
70
71  <!--NeedCopy-->
```

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.

Plugins management

October 7, 2023

Citrix Workspace app for Windows offers Plugins management capability that makes the Citrix Workspace app a single client app required on the end point to install and manage agents such as Secure Access Agent and End Point Analysis (EPA) plug-in.

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

Plugins management includes the following steps:

- Administrators must specify the agents required on end users' devices in the Global App Configuration Service. Administrators can specify Secure Access Agent and Endpoint Analysis (EPA) agent.
- Citrix Workspace app fetches the list of agents from Global App Configuration Service.
- Based on the list fetched from Global App Configuration service, Citrix Workspace app downloads the agent packages through the auto-update service. If the agent is not previously installed on the end point, Citrix Workspace app triggers the installation of the agent. If the agent is already installed, Citrix Workspace app triggers an update to the agent (if the version of the downloaded agent is higher than the installed version.)

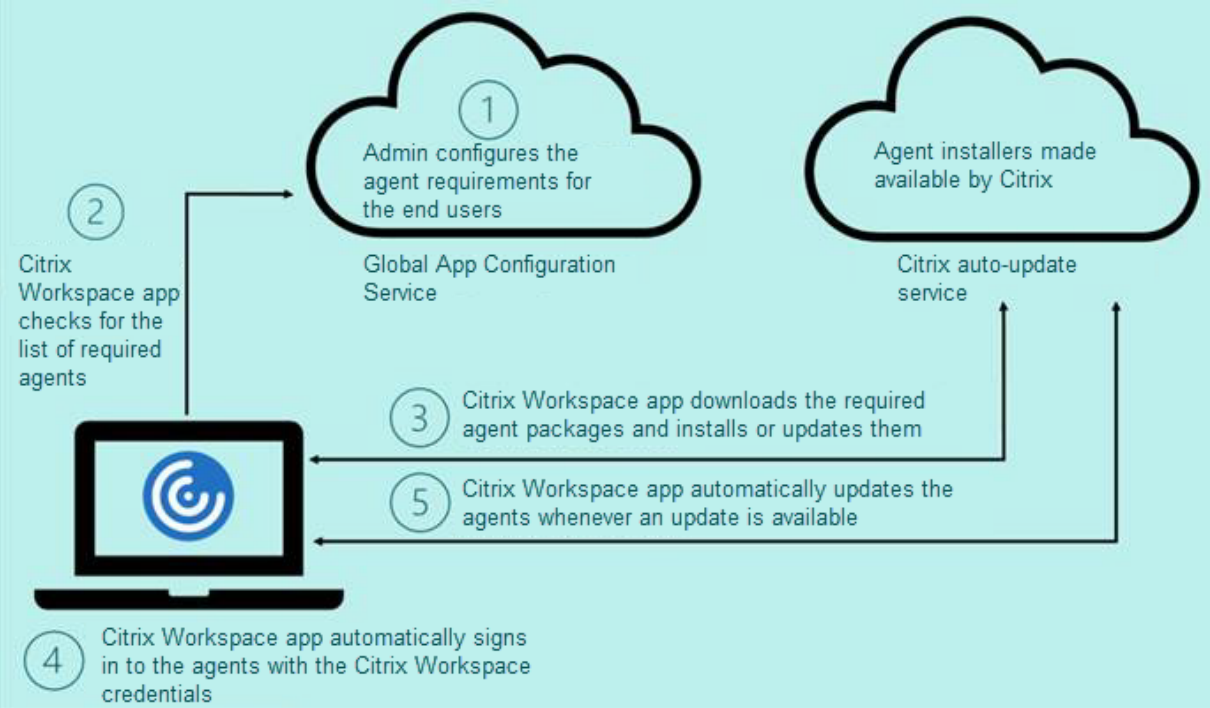
Citrix Workspace app ensures to automatically update the agents whenever an update is available in the future.

Citrix Workspace app automatically signs in to the agents with the Citrix Workspace credentials.

Notes:

- If the EPA and ZTNA plugins doesn't exists, the plugins are downloaded and installed while adding the store or account for the first time.
- If the store or account and plug-ins already exists and the installer contains a higher version, 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 Plugins management feature.

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

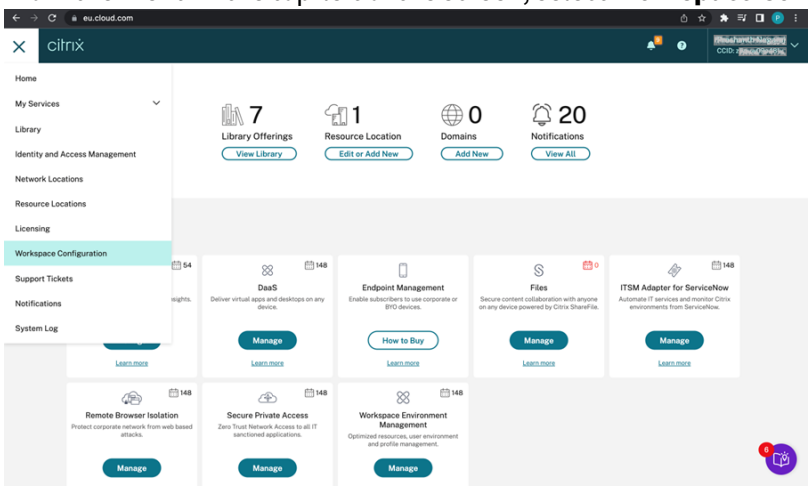
You can enable the Plugins management feature using the following methods:

- Using Global App Configuration service UI - Use this method to deploy the latest version of the client.
- Using Global App Configuration service API - Use this method to customize installation with parameters to control version, deployment modes, auto update intervals etc.

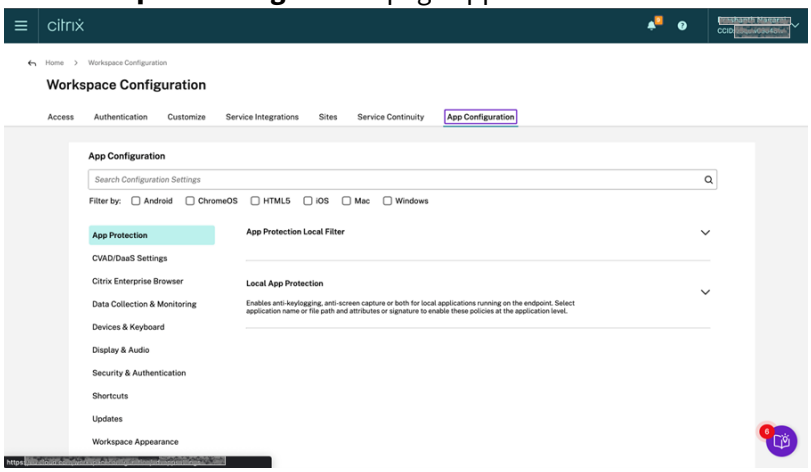
Enable Plugins management using Global App Configuration service UI

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

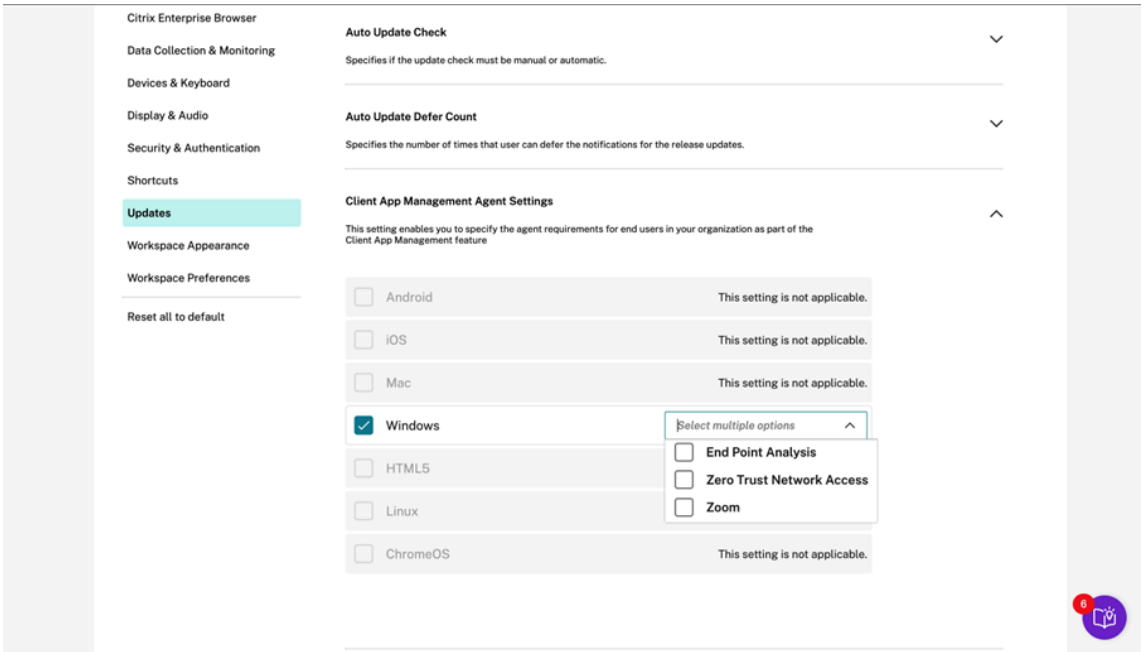
1. Sign in to Citrix Cloud.
2. From the menu in the top-left of the screen, select **Workspace Configuration**.



The **Workspace Configuration** page appears.



3. Click **App Configuration** tab.
4. Click **Updates**.
5. Ensure **Windows** check box is selected.
6. Select the required agents next to **Windows** from the **Client App Management Agent Settings** drop-down list.



Enable Plugins management using Gobal App Configuration service API

1. Configure and onboard settings in the Global app config service using API. For more information, see Map service URLs and configure settings.
2. Following Global App Configuration setting need to be onboarded for the store/account to onboard EPA and ZTNA/Secure Access Client:

```
{

    "serviceURL":
    {

        "url": "https://storefront.acme.com:443"
     }
 ,
    "settings":
    {

        "description": "Install and update plugins",
        "name": "Install and update plugins",
        "useForAppConfig": true,
        "appSettings":
        {

            "windows":
            [
                {

                    "assignedTo":
```



```
                    [
                        "AllUsersNoAuthentication"
                    ],
                    "category": "AutoUpdate",
                    "settings":
                    [
                        {

                            "name": "Auto Update plugins settings",
                            "value":
                            [
                                {

                                    "pluginId": "8A8AF6C0-11F6-4343-
                                       BA2D-A85A766170D4",
                                    "pluginName": "Citrix EPA Client",
                                    "pluginSettings":
                                    {

                                        "delayGroup": "Fast",
                                        "deployment Mode": "
                                           InstallAndUpdate",
                                        "detectRule": "UpgradeCode:{
37A181F7-870E-4BDF-B0EA-E3B4766119FE }
",
                                        "isBlocking": true,
                                        "isFTU": true,
                                        "maximumAllowedVersion": "
                                           23.8.1.24",
                                        "minimumAllowedVersion": "
                                           0.0.0.0",
                                        "stream": "Current",
                                        "upgradeToLatest": true
                                     }

                                 }
,
                                {

                                    "pluginId": "9A8AF6C0-11F6-4343-
                                       BA2D-A85A766170D5",
                                    "pluginName": "Citrix Secure Access
                                        Client",
                                    "pluginSettings":
                                    {

                                        "delayGroup": "Fast",
                                        "deployment Mode": "
                                           InstallAndUpdate",
                                        "detectRule": "UpgradeCode:{
F0ED53AB-11BE-4E9C-87E5-CD4A81DA2A4D }
",
                                        "isBlocking": false,
```



```
                                        "isFTU": true,
                                        "maximumAllowedVersion": "
                                            21.8.0.0",
                                        "minimumAllowedVersion": "
                                            0.0.0.0",
                                        "stream": "Current",
                                        "upgradeToLatest": true
                                    }

                                }
,
                                {

                                    "pluginId": "C03BAE37-F3AC-4D63-8
                                        BC1-3C9CD2BC9E8D",
                                    "pluginName": "WebEx VDI
                                        AutoUpgrade Plugin",
                                    "pluginSettings":
                                    {

                                        "delayGroup": "Fast",
                                        "deployment Mode": "
                                            InstallAndUpdate",
                                        "detectRule": "UpgradeCode:{
AA2AACDC-D30B-433F-A602-3E25975010A6 }
",
                                        "isBlocking": false,
                                        "isFTU": false,
                                        "maximumAllowedVersion": "
                                            3.1.0.24263",
                                        "minimumAllowedVersion": "0.0.0
                                            ",
                                        "stream": "Current",
                                        "upgradeToLatest": true
                                    }

                                }

                            ]
                        }

                    ],
                    "userOverride": false
                }

            ]
        }

    }

}


```



```
<!--NeedCopy-->
```

The following table lists the Plugins management settings schema, values, and description.

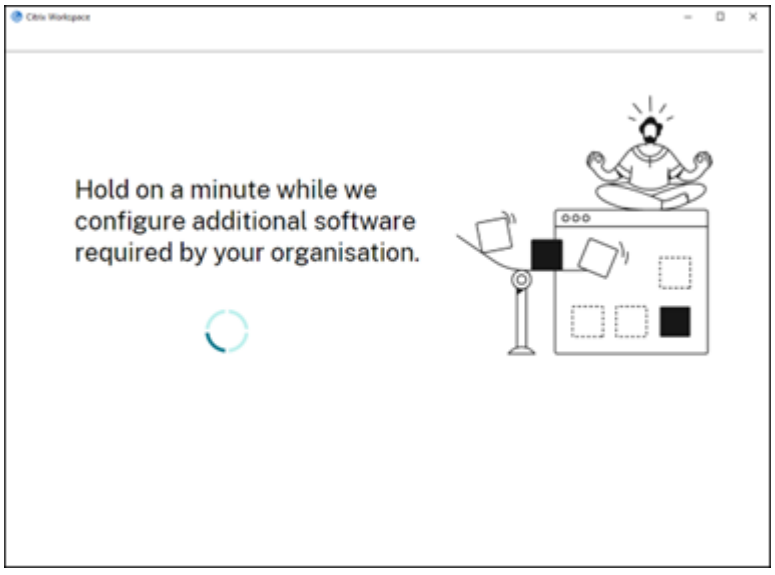
Schema setting	Value	Description
isBlocking	True or False	When the isBlocking parameter is set to true, the plug-in is considered mandatory, and the sign-in page appears only when the required plug-in is installed. Citrix recommends you set EPA as the mandatory plug-in.
pluginName		Friendly name for the plug-in. The pluginName can be modified.
pluginId		ID of the plug-in and must not be modified.
delayGroup	Fast, Medium, Slow	
Auto-update interval at which the plug-ins must be updated.		
deploymentMode	InstallAndUpdate/Update	InstallAndUpdate: Plugin can be freshly installed and updated with the new version.Update: Only update should be allowed, no fresh install.
None		No action is needed for this plug-in.
detectRule	Value must not be modified.	Checks if plug-in is already installed or not.
maximumAllowedVersion		Maximum allowed version of the plug-in.
minimumAllowedVersion		Minimum allowed version of the plug-in.
upgradeToLatest	True or False	

Schema setting	Value	Description
Must be set to false to support maximumAllowedVersion and minimumAllowedVersion. True: Latest version of the plug-in is considered during the update.		
Stream	Current	Must be set to Current to receive install or auto-update the plug-ins

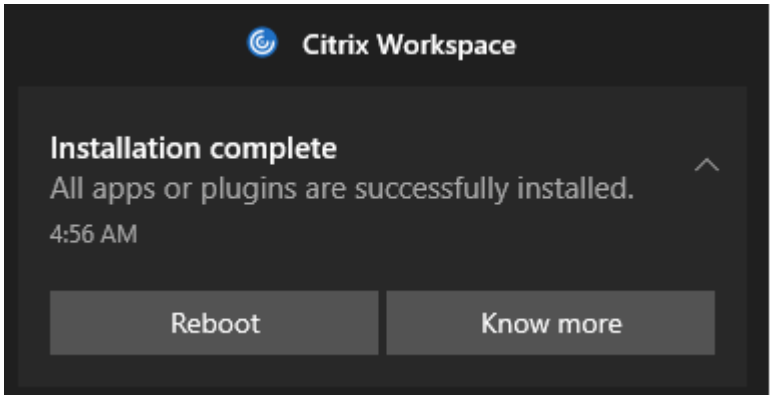
User workflow

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.

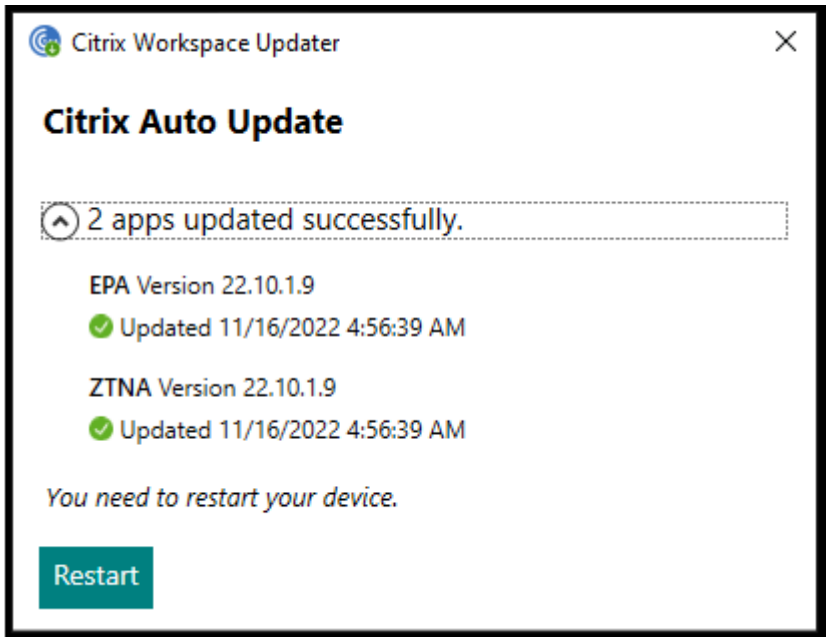
   The following message appears while installing the mandatory plug-ins:



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



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



Plugins management for Zoom plug-in

Download, install, and auto-update of Zoom plug-in is also supported and handled same way as EPA and ZTNA plug-ins.

The following Global App Configuration setting needs to be onboarded for the store/account to leverage this feature:

```
{

    "serviceURL":
    {

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



```
    "settings":
    {

        "description": "Install and update plugins",
        "name": "Install and update plugins",
        "useForAppConfig": true,
        "appSettings":
        {

            "windows":
            [
                {

                    "assignedTo":
                    [
                        "AllUsersNoAuthentication"
                    ],
                    "category": "AutoUpdate",
                    "settings":
                    [
                        {

                            "name": "Auto Update plugins settings",
                            "value":
                            [
                                {

                                    "pluginId": "1A4BB471-022C-4C87-
                                       BDCD-0B64FB42869C",
                                    "pluginName": "Zoom VDI AutoUpgrade
                                        Plugin",
                                    "pluginSettings":
                                    {

                                        "delayGroup": "Fast",
                                        "deploymentMode": "
                                           InstallAndUpdate",
                                        "detectRule": "UpgradeCode:{
34225638-14F3-4059-BE34-175AC9B35435 }
",
                                        "isBlocking": false,
                                        "isFTU": false,
                                        "maximumAllowedVersion": "
                                           5.11.2872",
                                        "minimumAllowedVersion": "0.0.0
                                           ",
                                        "stream": "Current",
                                        "upgradeToLatest": true
                                    }

                                }

                            ]
```



```
                            }

                        ],
                        "userOverride": false
                    }

                ]
            }

        }

 }


<!--NeedCopy-->
```

App experience

September 27, 2023

This section describes the following:

- Application delivery
- Improved virtual apps and desktops launch experience
- App preferences
- SaaS apps
- Data collection and monitoring

Application delivery

January 31, 2024

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

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

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

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

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

Configure self-service mode

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

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

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

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

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

Customize the app shortcut location using the Group Policy Object template

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

Using StoreFront account settings to customize app shortcut locations

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

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

- To use the category path in the Start menu, use UseCategoryAsStartMenuPath. Settings: "true" or "false"(default is true).

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

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

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

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

The section ends with the </account> tag.

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

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

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

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

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

An extended example for this section is:

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


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

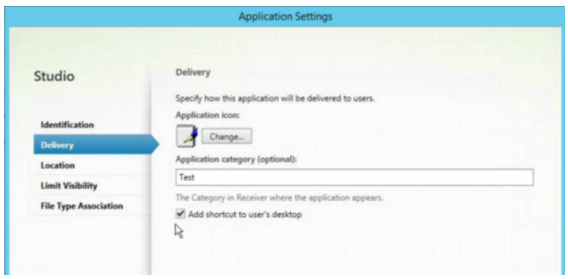
Using per-app settings in Citrix Virtual Apps and Desktops 7.x to customize app shortcut locations

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

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

To configure a per app publishing shortcut in XenApp 7.6:

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



Reducing enumeration delays or digitally signing application stubs

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

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

This functionality involves several steps:

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

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

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

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

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

1. On a client machine, create stub executables for all apps. To accomplish create stub executables, add all the applications to the machine using Citrix Workspace app. Citrix Workspace app generates the executables.
2. Harvest the stub executables from `%APPDATA%\Citrix\SelfService`. You only need the .exe files.
3. Copy the executables to a network share.
4. For each client machine that is locked down, set the following registry keys:

    a) Reg add `HKEY_LOCAL_MACHINE\Software\Citrix\Dazzle` /v CommonStubDirectory /t REG_SZ /d "\\ShareOne\WorkspaceStubs"
    b) Reg add `HKEY_LOCAL_MACHINE\Software\Citrix\Dazzle` /v

c) `CopyStubsFromCommonStubDirectory` /t REG_SZ /d “true”. It’s also possible to configure these settings on HKEY_CURRENT_USER if you prefer. HKEY_CURRENT_USER has preference over HKEY_LOCAL_MACHINE.
d) Exit and restart Citrix Workspace app for the changes to take effect.

Example use cases:

This topic provides use cases for app shortcuts.

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

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

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

No app shortcuts in the Start menu

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

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

All app shortcuts in the Start menu or on the Desktop

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

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

Per app settings in XenApp 6.5 or 7.x

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

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

Apps in category folders or in specific folders

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

If you want the application shortcuts Citrix Workspace app places in the start menu to be shown in their associated category (folder).	configure Citrix Workspace app with UseCategoryAsStartMenuPath=True.

If you want the applications that Citrix Workspace app puts in the Start menu to be in a specific folder.	configure Citrix Workspace app with StartMenuDir=the name of the Start menu folder name.

Remove apps on logoff or exit

If you don't want users to see apps while another user share the end point, you can remove the apps when the user logs off and exits.

If you want Citrix Workspace app to remove all apps on logoff.	configure Citrix Workspace app with RemoveAppsOnLogoff=True.
If you want Citrix Workspace app to remove apps on exit.	configure Citrix Workspace app with RemoveAppsOnExit=True.

Configuring Local App Access applications

When configuring Local App Access applications:

- To specify that a locally installed application must be used instead of an application available in Citrix Workspace app, append the text string KEYWORDS:prefer="pattern."This feature is referred to as Local App Access.

  Before you install an application on a user's computer, Citrix Workspace app searches for the specified patterns to determine if the application is installed locally. If it is, Citrix Workspace app subscribes the application and does not create a shortcut. When the user starts the application from the Citrix Workspace app window, Citrix Workspace app starts the locally installed (preferred) application.

  If a user uninstalls a preferred application outside of Citrix Workspace app, the application is unsubscribed during the next Citrix Workspace app refresh. If a user uninstalls a preferred application from the Citrix Workspace app dialog, Citrix Workspace app unsubscribes the application but does not uninstall it.

> **Note:**
>
> The keyword prefer is applied when Citrix Workspace app subscribes an application. Adding the keyword after the application is subscribed has no effect.

You can specify the prefer keyword multiple times for an application. Only one match is needed to apply the keyword to an application. The following patterns can be used in any combination:

- To specify that a locally installed application must be used instead of an application available in Citrix Workspace app, append the text string KEYWORDS:prefer="pattern". This feature is referred to as Local App Access.

  Before you install an application on a user's computer, Citrix Workspace app searches for the specified patterns to determine if the application is installed locally. If it is, Citrix Workspace app subscribes the application and does not create a shortcut. When the user starts the application from the Citrix Workspace app dialog, Citrix Workspace app starts the locally installed (preferred) application.

  If a user uninstalls a preferred application outside of Citrix Workspace app, the application is unsubscribed during the next Citrix Workspace app refresh. If a user uninstalls a preferred application from the Citrix Workspace app, Citrix Workspace app unsubscribes the application but does not uninstall it.

> **Note:**
>
> The keyword prefer is applied when Citrix Workspace app subscribes an application. Adding the keyword after the application is subscribed has no effect.

You can specify the 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
\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

For information about other keywords, see "Additional recommendations"in Optimize the user experience section in the StoreFront documentation.

vPrefer launch

In earlier releases, you can specify that the instance of an app installed on the VDA (referred to as local instance in this document) must be launched in preference to the published application by setting the KEYWORDS:prefer="application"attribute in **Citrix Studio**.

Starting with Version 4.11, in a double-hop scenario (where Citrix Workspace app is running on the VDA that hosts your session), you can now control whether Citrix Workspace app launches:

- the local instance of an application installed on the VDA (if available as a local app) or
- a hosted instance of the application.

vPrefer is available on StoreFront Version 3.14 and Citrix Virtual Desktops 7.17 and later.

When you launch the application, Citrix Workspace app reads the resource data present on the StoreFront server and applies the settings based on the **vprefer** flag at the time of enumeration. Citrix Workspace app searches for the application's installation path in the Windows registry of the VDA. If present, launches the local instance of the application. Otherwise, a hosted instance of the application is launched.
If you launch an application that is not on the VDA, Citrix Workspace app launches the hosted application. For more information on how StoreFront handled the local launch, see Control of local application launch on published desktops in the Citrix Virtual Apps and Desktops documentation.

If you do not want the local instance of the application to be launched on the VDA, set the **LocalLaunchDisabled** to **True** using the PowerShell on the Delivery Controller. For more information, see the Citrix Virtual Apps and Desktops documentation.

This feature helps to launch applications faster, thereby providing a better user experience. You can configure it by using the Group Policy Object (GPO) administrative template. By default, vPrefer is enabled only in a double-hop scenario.

> **Note:**
>
> When you upgrade or install Citrix Workspace app for the first time, add the latest template files to the local GPO. For more information on adding template files to the local GPO, see Group Policy Object administrative template. For an upgrade, the existing settings are retained while importing the latest files.

1. Open the Citrix Workspace app GPO administrative template by running gpedit.msc.
2. Under the **Computer Configuration** node, go to **Administrative Template** > **Citrix Component** > **Citrix Workspace** > **SelfService**.
3. Select the **vPrefer** policy.
4. Select **Enabled**.
5. From the **Allow apps** drop-down list, select one of the following options:

- **Allow all apps**: This option launches the local instance of all apps on the VDA. Citrix Workspace app searches for the installed application, including the native Windows apps such as Notepad, Calculator, WordPad, Command prompt. It then launches the application on the VDA instead of the hosted app.
- **Allow installed apps**: This option launches the local instance of the installed app on the VDA. If the app is not installed on the VDA, it launches the hosted app. By default, **Allow installed apps** is selected when the **vPrefer** policy is set to **Enabled**. This option excludes the native Windows operating system applications like Notepad, Calculator, 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:

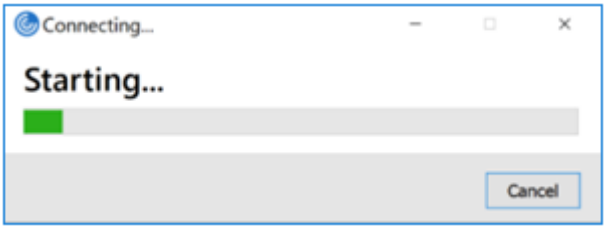
- Workspace for web does not support this feature.

Improved virtual apps and desktops launch experience

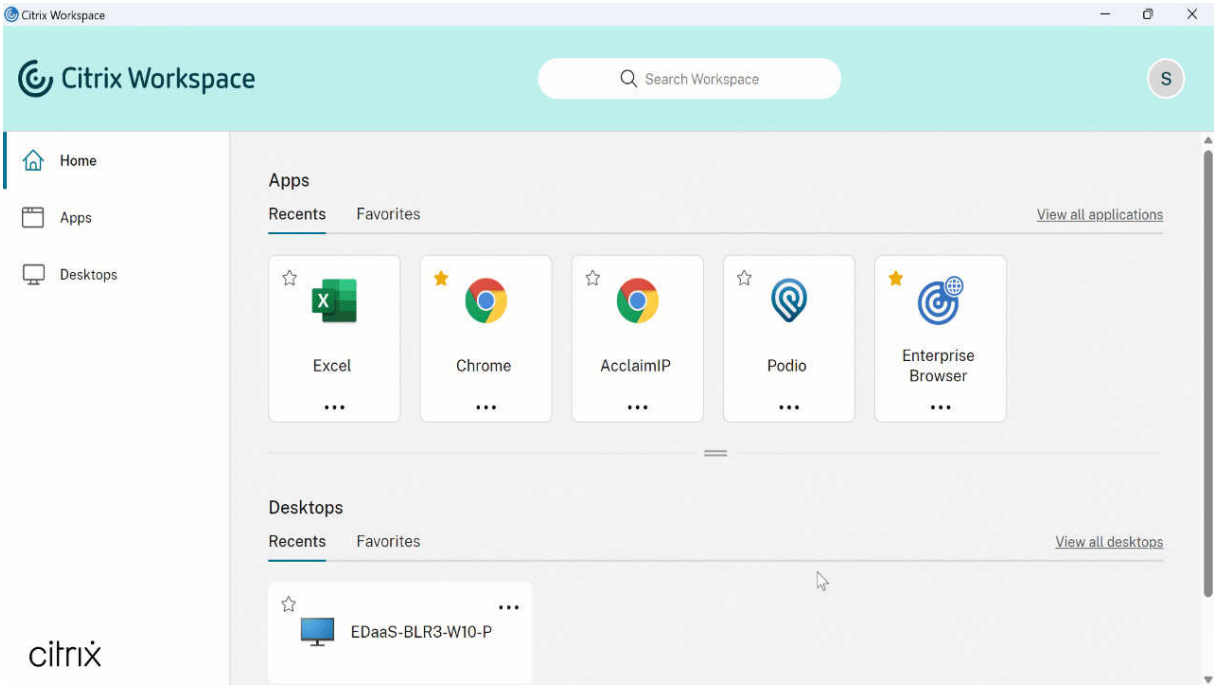
October 7, 2023

> **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 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.



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

October 7, 2023

Advanced Preferences sheet

You can customize **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.

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

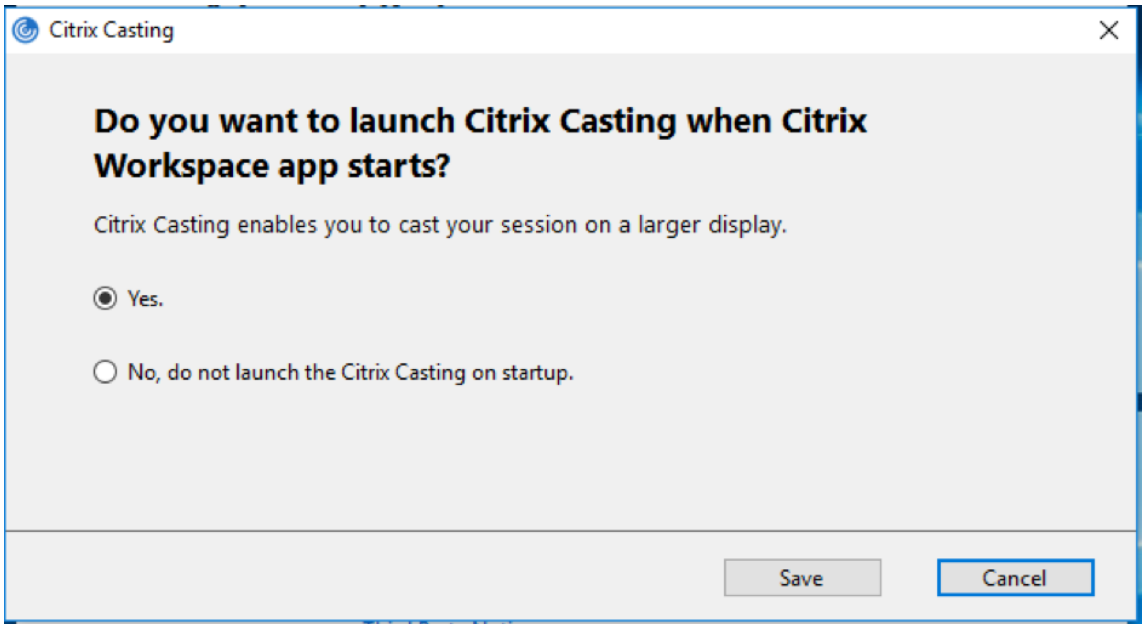
> **Note:**
>
> You can hide all or part of the Advanced Preferences sheet. For more information, see Advanced Preferences sheet.

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.

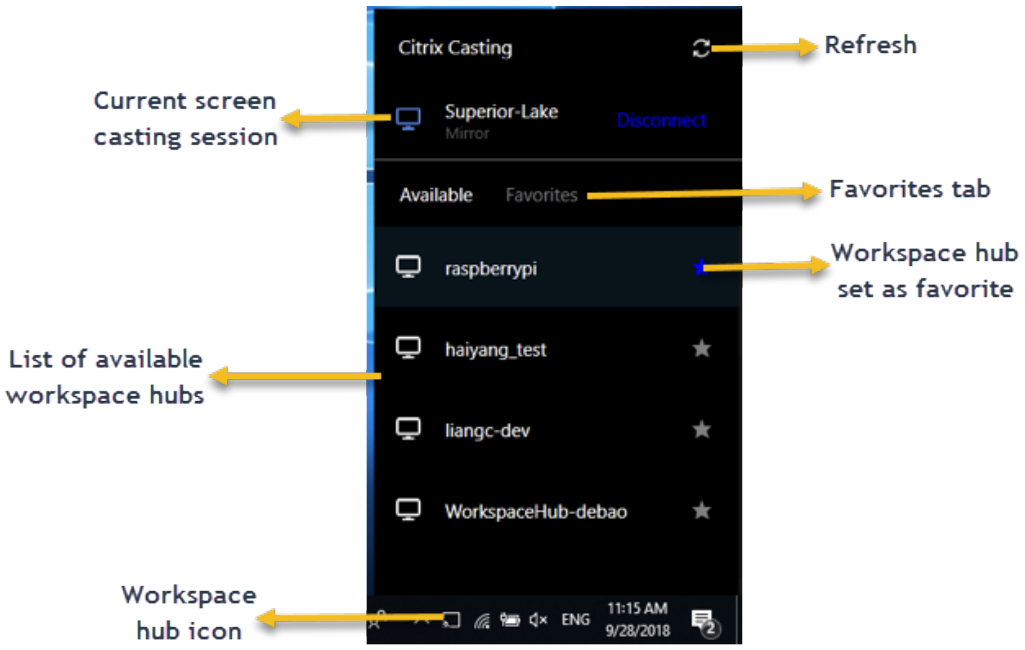
2. Select the workspace hub to cast your screen and choose one of the following:

   - **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.

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

October 7, 2023

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 Workspace configuration, see Workspace configuration in Citrix Cloud.

Data collection and monitoring

December 7, 2023

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 to **Off**.

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

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

> **Note:**
>
> - 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)

Data collected	Description	What we use it for
Configuration and usage data	The Citrix Customer Experience Improvement Program (CEIP) gathers configuration and usage data from Citrix Workspace app for Windows and automatically sends the data to Citrix and Google Analytics.	This data helps Citrix improve the quality, functionality, and performance of the Citrix Workspace app, appropriately allocate resources for product development purposes, and maintain service levels and manage staffing and infrastructure investment.

Data collected

As noted above, Citrix collects Citrix Workspace app configuration and usage data to improve the quality, functionality, and performance of Workspace App, and to allow Citrix to appropriately allocate resources for product development purposes, as well as to maintain service levels and manage staffing and infrastructure investment. The data is used and analyzed in aggregated form only. No user or their machine is singled-out and no analysis is performed on specific end users based on the CEIP data.

The specific CEIP data elements collected by Google Analytics and 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/Properties	Citrix Virtual Apps and Desktops Session Launch Status	Virtual app/desktop name	Auto-update Status
Connection Lease Details	StoreFront to Workspace URL Migration Feature Usage	Citrix Enterprise Browser Usage	Auto-update channel
Inactivity Timeout Details	Citrix Enterprise Browser Version		

> **Note:**
>
> Starting with version 2206, the Citrix Workspace app doesn't collect any CEIP data from users located in the European Union (EU), European Economic Area (EEA), Switzerland, and United Kingdom (UK). Update your Citrix Workspace app if you wish to take advantage of this functionality.

Data Collection Preferences

Starting with version 2205, both users and administrators can stop sending CEIP data (except for the two data elements which can be blocked as specified in the Note below) by following the below steps.

1. Right-click the Citrix Workspace app icon from the notification area.
2. Select **Advanced Preferences**.
   The **Advanced Preferences** dialog appears.
3. Select **Data Collection**.
4. Select **No, Thanks** to disable CEIP or to forego participation.
5. Click **Save**.

You can also navigate to the following registry entry as an administrator and set the value as suggested:

Path: `HKEY_LOCAL_MACHINE\ SOFTWARE\Citrix\ICA Client\CEIP`

Key: `Enable_CEIP`

Value: `False`

> **Note:**
>
> Once you select **No Thanks** or set the `Enable_CEIP` key to `False`, you can also stop sending the final two CEIP data elements, that is, Operating System and Citrix Workspace app version, by navigating to the following registry entry and set the value:

Path: `HKEY_LOCAL_MACHINE\ SOFTWARE\Citrix\ICA Client\CEIP`

Key: `DisableHeartbeat`

Value: `True`

Additional information

Citrix handles your data according to the terms of your contract with Citrix, and protect it as specified in the Citrix Services Security Exhibit. Citrix Services Security Exhibit is available on the Citrix Trust Center.

<

>

>

<

Security and authentication

October 7, 2023

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

October 7, 2023

App Protection

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

Improved ICA file security

This feature provides enhanced security while handling ICA files during a virtual apps and desktops session launch.

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

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

Configuration

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

StoreFront Version	Attribute
2.x	pluginassistant
3.x	protocolHandler

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

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

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

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

Using the GPO:

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

1. Open the Citrix Workspace app Group Policy Object administrative template by running `gpedit.msc`.

2. Under the **Computer Configuration** node, go to **Administrative Templates** > **Citrix Components** > **Citrix Workspace** > **Client Engine**.
3. Select the **Secure ICA file session launch** policy and set it to **Enabled**.
4. Click **Apply** and **OK**.

Using the Global App Config Service:

You can use Global App Config Service from Citrix Workspace app 2106.

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

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

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

Using workspace for web:

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

Run the PowerShell module. See Configure DisallowICADownload.

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

Inactivity Timeout for Workspace Sessions

Admins can configure the inactivity timeout value to specify the amount of idle time allowed before the users automatically sign out of the Citrix Workspace session. You're automatically signed out of Workspace if the mouse, keyboard, or touch is idle for the specified interval of time. The inactivity timeout doesn't affect the active virtual apps and desktops sessions or Citrix StoreFront stores.

The inactivity timeout value can be set starting from a 1 minute to 1,440 minutes. By default, the inactivity timeout isn't configured. Admins can configure the inactivityTimeoutInMinutes property by using a PowerShell module. Click here to download the PowerShell modules for Citrix Workspace Configuration.

The end-user experience is as follows:

- A notification appears in your session window three minutes before you're signed out, with an option to stay signed in, or sign out.
- The notification appears only if the configured inactivity timeout value is greater than or equal to five minutes.
- Users can click **Stay signed in** to dismiss the notification and continue using the app, in which case the inactivity timer is reset to its configured value. You can also click **Sign out** to end the session for the current store.

> **Note:**
>
> Admins can configure the inactivity timeout only for Workspace (cloud) sessions.

Secure communications

October 11, 2023

To secure the communication between Citrix Virtual Apps and Desktops server and Citrix Workspace app, you can integrate your Citrix Workspace app connections using a range of secure technologies such as the following:

- Citrix Gateway: For information, see the topics in this section and the Citrix Gateway, and StoreFront documentation.
- A firewall: Network firewalls can allow or block packets based on the destination address and port.
- Transport Layer Security (TLS) versions 1.0 through 1.3 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

Source	Type	Port	Details
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 use of TLS: We recommend that you use TLS for connections using untrusted networks, including the Internet.
- Enforce use of FIPS (Federal Information Processing Standards): Approved cryptography and follow the recommendations in NIST SP 800-52. These options are disabled by default.
- Enforce use of a specific version of TLS and specific TLS cipher suites: Citrix supports the TLS 1.0, TLS 1.1, and TLS 1.2 protocols.
- Connect only to specific servers.
- Check for revocation of the server certificate.
- Check for a specific server-certificate issuance policy.
- Select a particular client certificate, if the server is configured to request one.

Citrix Workspace app for Windows supports the following cipher suites for TLS 1.2 protocol:

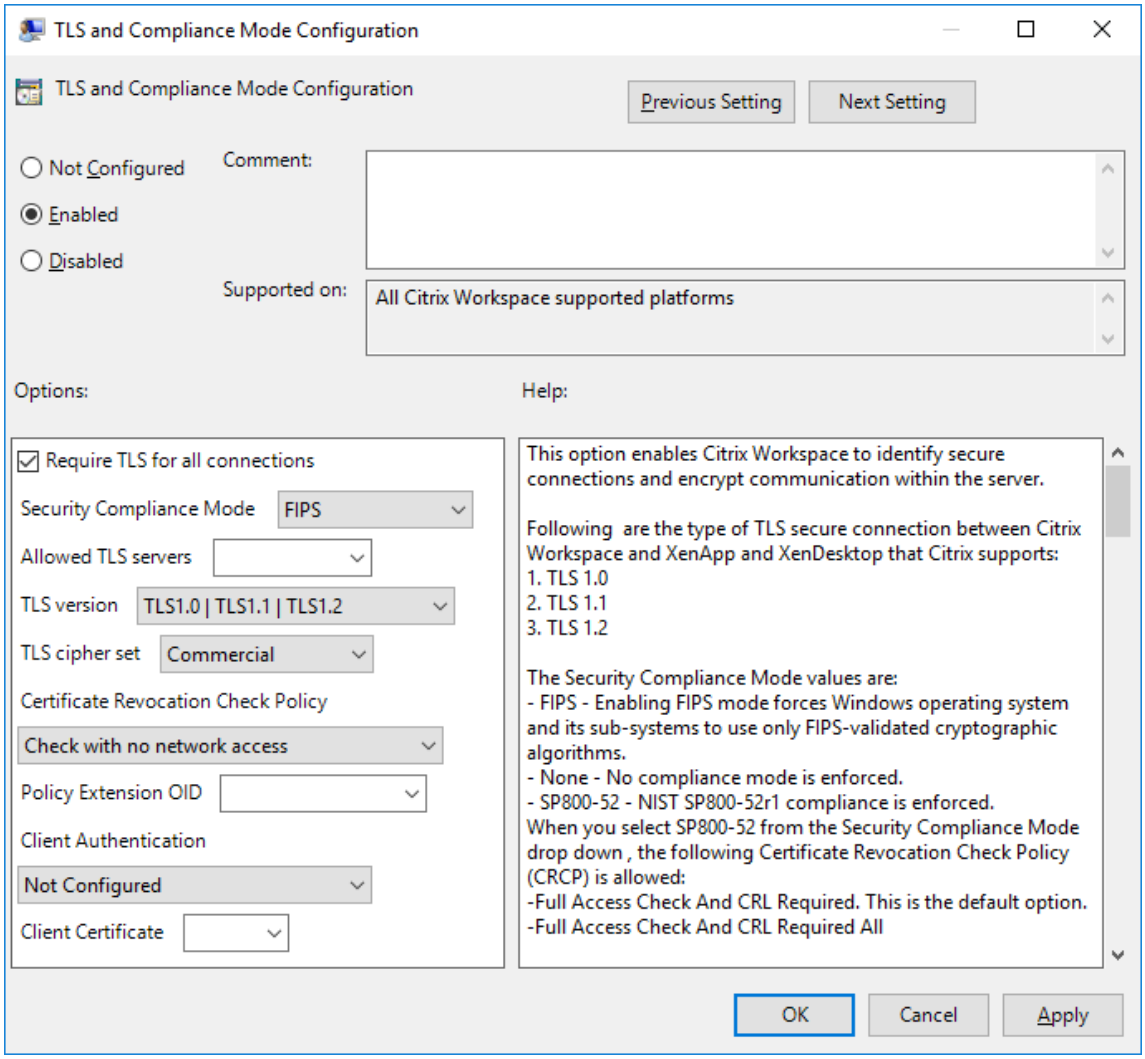
- TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384
- TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384
- TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA

For information on the supported cipher suites, see the Knowledge Center article CTX250104.

> **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. This option is recommended only if there is a business requirement for TLS 1.0 for compatibility.
- **TLS 1.1 or TLS 1.2** - Use this option to ensure that the 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). For more information, see Knowledge Center article CTX250104.

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.

For information on the internal and external network connections matrix, see the Knowledge Center article CTX250104.

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, the server address can be specifically trusted using the **Address** setting. The server address must be comma-separated list of servers supporting the use of wildcards, for example, `cps*.citrix.com`.

To enable trusted server configuration using Group Policy Object administrative template

Prerequisite:

Exit from the Citrix Workspace app components including the Connection Center.

1. Open the Citrix Workspace app GPO administrative template by running gpedit.msc.
2. Under the **Computer Configuration** node, go to **Administrative Templates** > **Citrix Components** > **Citrix Workspace** > **Network Routing** > **Configure trusted server configuration**.
3. Select **Enabled** to force Citrix Workspace app for region identification.
4. Select **Enforce trusted server configuration**. This option forces the client to perform the identification using a trusted server.
5. From the **Windows internet zone** drop-down menu, select the client-server address. This setting is applicable only to the Windows Trusted Site zone.
6. In the **Address** field, set the client-server address for the trusted site zone other than the Windows. You can use a comma-separated list.
7. Click **OK** and **Apply**.

When this policy is enabled and the server is not in the trusted region, the connection is prevented, and an error message is displayed.
The identified server must be added to the Windows **Trusted Sites zone** for the connection to succeed. For example, add the server as either, http:// or https:// for SSL connections.

> **Note:**
>
> For SSL connections, the certificate common name must be trusted. For non-SSL connections all servers that are contacted must be individually trusted.

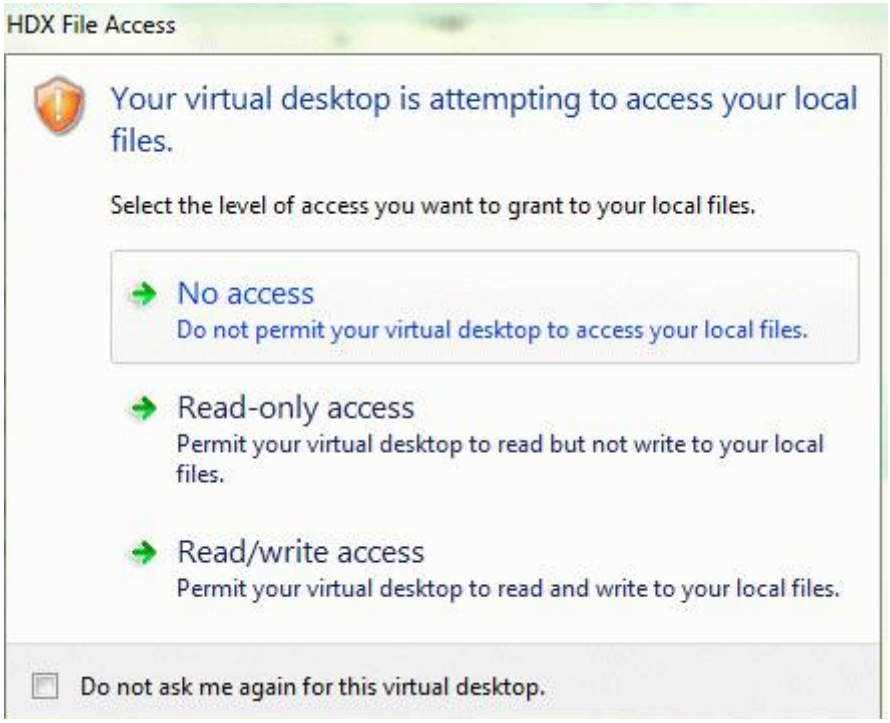
Also, ensure that the internal StoreFront FQDN is added to the Local Intranet zone or Trusted sites zones. For information, see **Modify the Internet Explorer settings** in Authenticate section.

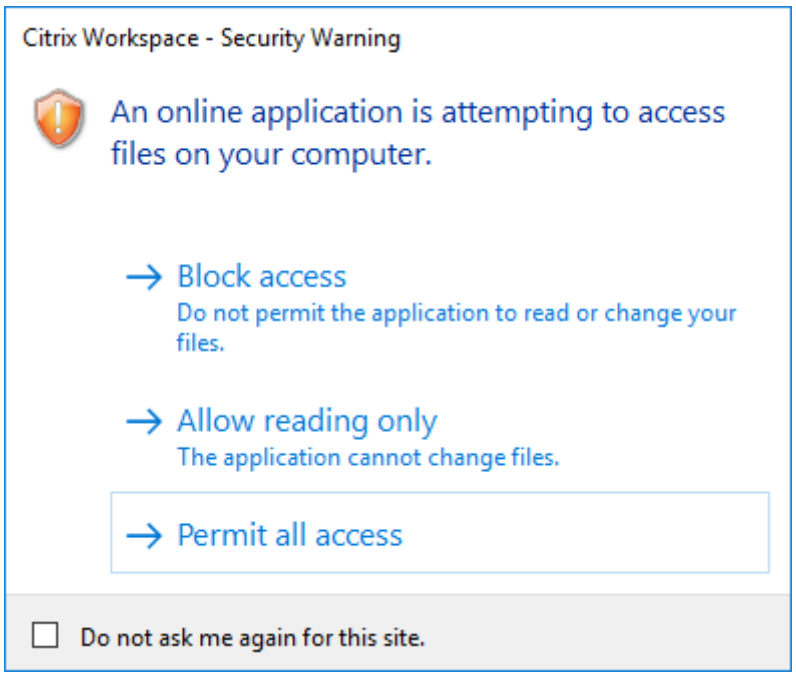
Client selective trust

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
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.

ICA file signing

The ICA file signing helps protect you from an unauthorized application or desktop launch. Citrix Workspace app verifies that a trusted source generated the application or desktop launch based on an administrative policy and protects against launches from untrusted servers. You can configure ICA file signing using the Group policy objects administrative template or StoreFront. The ICA file signing feature isn't enabled by default.

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

Configure ICA file signature

> **Note:**
>
> If the CitrixBase.admx\adml isn't added to the local GPO, the **Enable ICA File Signing** policy might not be present.

1. Open the Citrix Workspace app Group Policy Object administrative template by running gpedit.msc
2. Under the **Computer Configuration** node, go to **Administrative Templates** > **Citrix Components**.
3. Select **Enable ICA File Signing** policy and select one of the options as required:

a) Enabled - Indicates that you can add the signing certificate thumbprint to the allow list of trusted certificate thumbprints.
b) Trust Certificates - Click **Show** to remove the existing signing certificate thumbprint from the allow list. You can copy and paste the signing certificate thumbprints from the signing certificate properties.
c) Security policy - Select one of the following options from the menu.
    i. Only allow signed launches (more secure): Allows only signed application and desktop launches from a trusted server. A security warning appears when there's an invalid signature. The session launch fails because of non-authorization.
    ii. Prompt user on unsigned launches (less secure) - A message prompt appears when an unsigned or invalidly signed session is launched. You can choose to either continue the launch or cancel the launch (default).

4. Click **Apply** and **OK** to save the policy.
5. Restart the Citrix Workspace app session for the changes to take effect.

To select and distribute a digital signature certificate:

When selecting a digital signature certificate, we recommend you choose from the following priority list:

1. Buy a code-signing certificate or SSL signing certificate from a public Certificate Authority (CA).
2. If your enterprise has a private CA, create a code-signing certificate or SSL signing certificate using the private CA.
3. Use an existing SSL certificate.
4. Create a root CA certificate and distribute it to user devices using GPO or manual installation.

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.

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

February 2, 2024

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.

Domain pass-through (single sign-on) authentication

Domain pass-through (single sign-on or 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:**
>
> If you disable the **Enable MPR notifications for the System** policy in the Group Policy Object template, the domain pass-through (single sign-on) authentication feature isn't supported on Windows 11.
> This feature is available from Citrix Workspace app for Windows version 2012 and later.

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.

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.

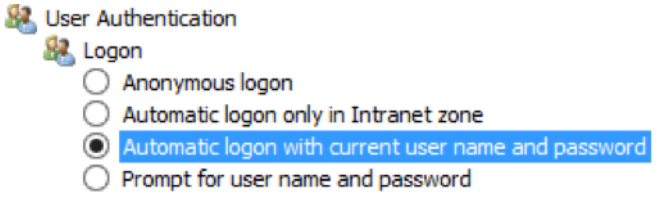
Configure XML trust services on the Delivery Controller

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.

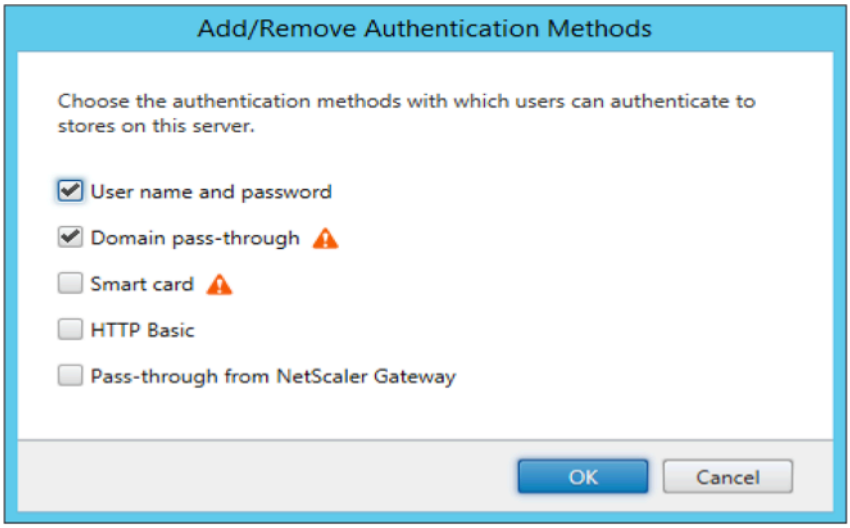
1. Download and place the Citrix Workspace app installation file (CitrixWorkspaceApp.exe) on a suitable network share. It must be accessible by the target machines you install Citrix Workspace app on.
2. Get the `CheckAndDeployWorkspacePerMachineStartupScript.bat`template from the Citrix Workspace app 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 `CheckAndDeployWorkspacePerMac.bat` as a startup script. For more information on deploying the startup scripts, see the Active Directory section.
5. In the **Computer Configuration** node, go to **Administrative Templates > Add/Remove Templates** to add the `receiver.adml` file.
6. After adding the `receiver.adml` template, go to **Computer Configuration** > **Administrative Templates** > **Citrix Components** > **Citrix Workspace** > **User authentication**. For more information about adding the template files, see Group Policy Object administrative template.

7. Select the **Local user name and password** policy and set it to **Enabled**.
8. Select **Enable pass-through authentication** and click **Apply**.
9. Restart the machine for the changes to take effect.

Configure single sign-on on StoreFront

StoreFront configuration

1. Launch **Citrix Studio** on the StoreFront server and select **Stores** > **Manage Authentication Methods - Store**.
2. Select **Domain pass-through**.



Authentication tokens

Authentication tokens are encrypted and stored on the local disk so that you don't need to reenter your credentials when your system or session restarts. Citrix Workspace app provides an option to disable the storing of authentication tokens on the local disk.

For enhanced security, we now provide a Group Policy Object (GPO) policy to configure the authentication token storage.

> **Note:**
>
> This configuration is applicable only in cloud deployments.

To disable storing of authentication tokens using the Group Policy Object (GPO) policy:

1. Open the Citrix Workspace app Group Policy Object administrative template by running `gpedit.msc`.

2. Under the **Computer Configuration** node, go to **Administrative Templates** > **Citrix Components** > **SelfService**.
3. In the **Store authentication tokens** policy, select one of the following:
    - Enabled: Indicates that the authentication tokens are stored on the disk. By default, set to Enabled.
    - Disabled: Indicates that the authentication tokens aren't stored on the disk. Reenter your credentials when your system or session restarts.
4. Click **Apply** and **OK**.

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`.

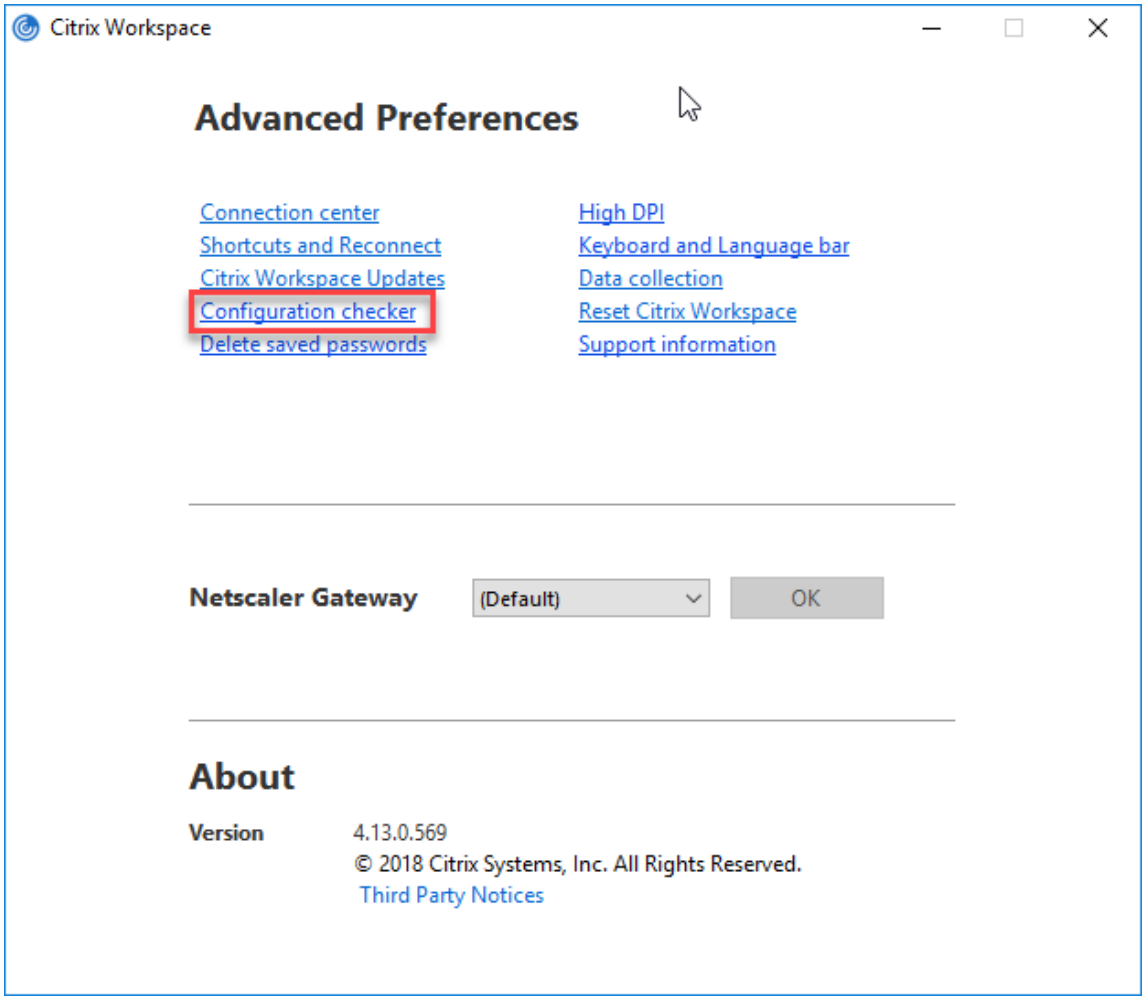
You can configure this setting using the Global App Configuration service in one of the following methods:

- 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 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. 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. This diagnostic test helps to eliminate one of the many possible causes

for slow resource enumeration, that is the beacon not being available. To run the test, right-click the Citrix Workspace app in the notification area and select **Advanced Preferences** > **Configuration Checker**. Select the **Beacon checker** option from the list of Tests and click **Run**.

The test results can be any of the following:

- Reachable –Citrix Workspace app is successfully able to contact the beacon.
- Not reachable - Citrix Workspace app is unable to contact the beacon.
- Partially reachable - Citrix Workspace app can contact the beacon intermittently.

> **Note:**
>
> - The test results aren't applicable on workspace for web.
> - The test results can be saved as reports. The default format for the report is .txt.

Domain pass-through (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`

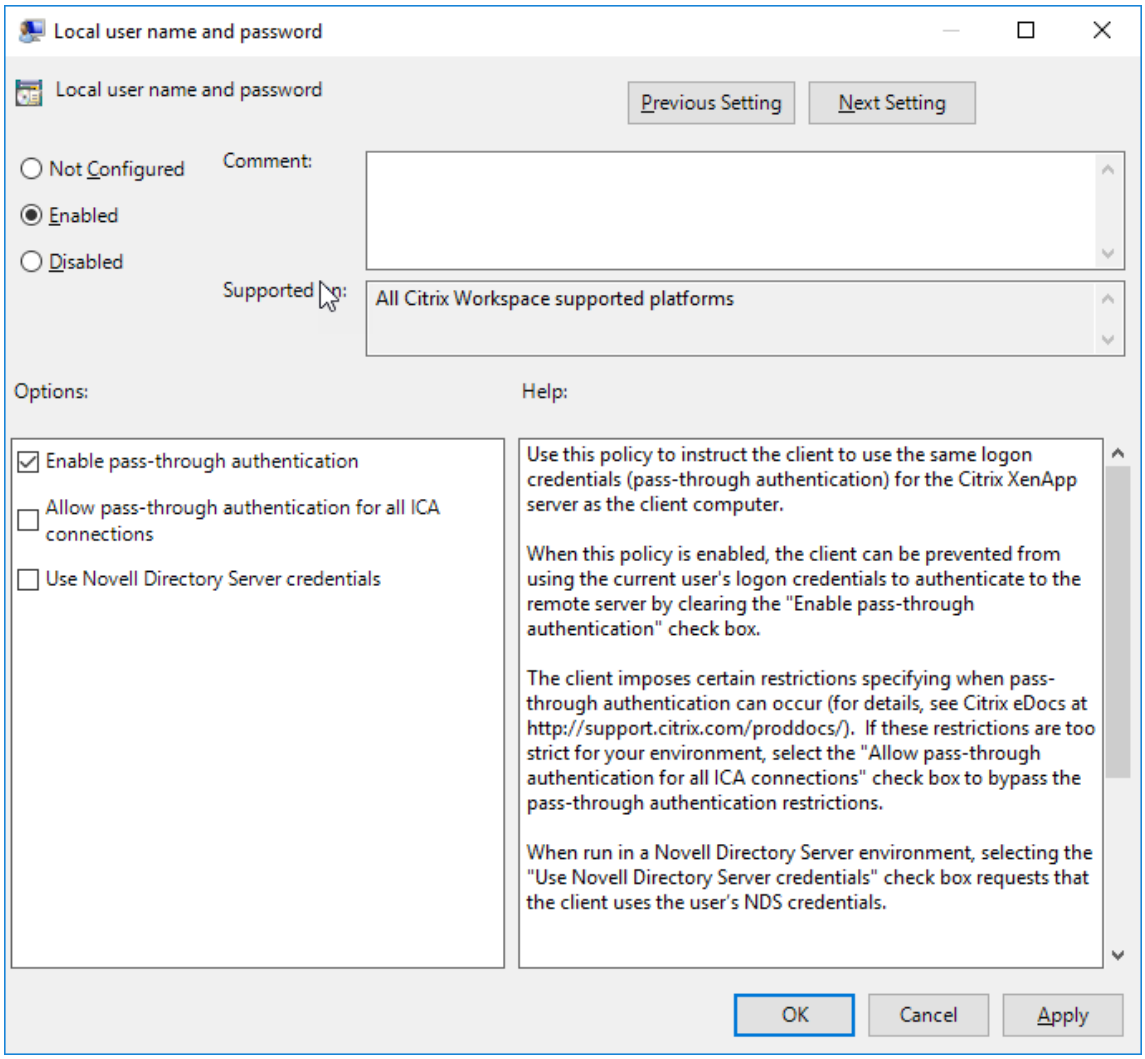
  This option installs the single sign-on component on the domain-joined computer, enabling your workspace to authenticate to StoreFront using IWA (Kerberos). The single sign-on component stores the smart card PIN, used by the HDX engine when it remotes the smart card hardware and credentials to Citrix 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.

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 99 or later installed.

For complete details and instructions about configuring conditional access policies with Azure Active Directory, see **Azure AD Conditional Access documentation** at *Docs.microsoft.com/en-us/azure/active-directory/conditional-access/*.

> **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.

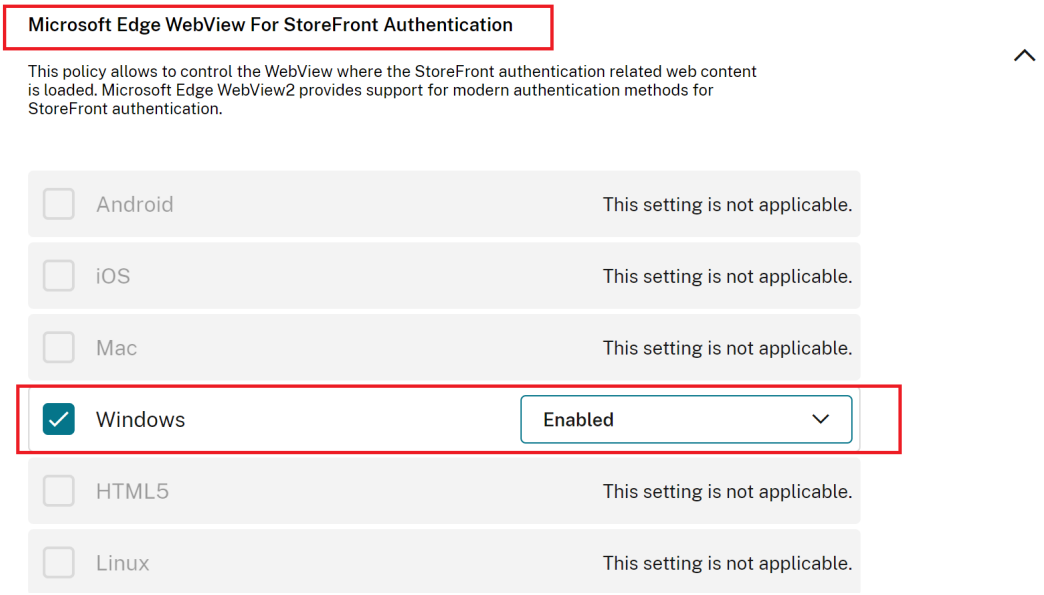
> **Note:**
>
> Ensure that the Microsoft Edge WebView2 Runtime version is 102 or later.

You can enable modern authentication methods for StoreFront storess 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 **Workspace Configuration** 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.

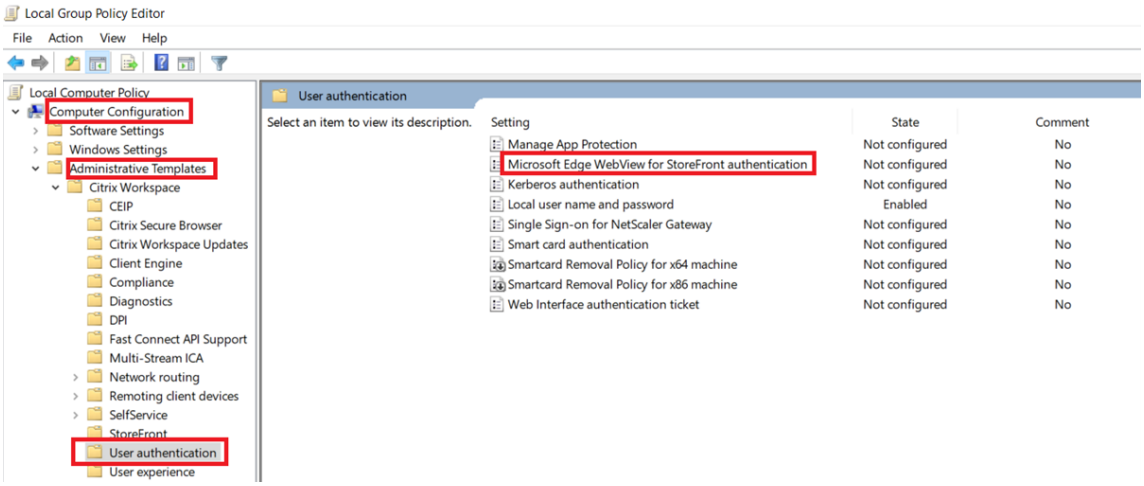


> **Note:**
>
> If you select **Disabled** next to **Windows** from the **Microsoft Edge WebView for Storefront Authentication** drop-down list, Internet Explorer WebView is used within the Citrix Workspace app. As a result, the modern authentication methods for Citrix Storefront stores are not supported.

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.

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 99 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** at _Docs.microsoft.com/en-us/windows/security/identity-protection/hello-for-business/hello-cert-trust-policy-settings.

   > **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** at *Docs.microsoft.com/en-us/azure/active-directory/authentication/howto-authentication-passwordless-security-key*.

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 at *Docs.microsoft.com/en-us/azure/active-directory-domain-services/overview*. For information about how to connect Azure Active Directory to Citrix Cloud, see Connect Azure Active Directory to Citrix Cloud.

Smart card

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

- **Pass-through authentication (single sign-on)** - Pass-through authentication captures the smart card credentials when users log on to Citrix Workspace app. Citrix Workspace app uses the captured credentials as follows:
  - Users of domain-joined devices who log on to Citrix Workspace app using the smart card can start virtual desktops and applications without needing to reauthenticate.
  - Citrix Workspace app running on non-domain joined devices with the smart card credentials must type their credentials again to start a virtual desktop or application.

  Pass-through authentication requires configuration both on StoreFront and Citrix Workspace app.
- **Bimodal authentication** - Bimodal authentication offers users a choice between using a smart card and typing the user name and password. This feature is effective when you can't use the smart card. For example, the logon certificate has expired. Dedicated stores must be set up per site to allow Bimodal authentication, using the **DisableCtrlAltDel** method set to **False** to allow smart cards. Bimodal authentication requires StoreFront configuration.

  Using the Bimodal authentication, the StoreFront administrator can allow both user name and password and smart card authentication to the same store by selecting them in the StoreFront console. See StoreFront documentation.
- **Multiple certificates** - Multiple certificates can be availed for a single smart card and if multiple smart cards are in use. When you insert a smart card in a card reader, the certificates are applicable to all applications running on the user device, including Citrix Workspace app.
- **Client certificate authentication** - Client certificate authentication requires Citrix Gateway and StoreFront configuration.
  - For access to StoreFront through Citrix Gateway, you must reauthenticate after removing the smart card.
  - When the Citrix Gateway SSL configuration is set to **Mandatory client certificate authentication**, operation is more secure. However, mandatory client certificate authentication isn't compatible with bimodal authentication.
- **Double hop sessions** - If a double-hop is required, a connection is established between Citrix Workspace app and the user's virtual desktop.

- **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
<!--NeedCopy-->
```

To disable fast smart card logon on Citrix Workspace app:

To disable fast smart card logon on Citrix Workspace app, remove the SmartCardCryptographicRedirecti parameter from the **default.**ica file of the associated StoreFront site.

For more information, see smart-cards.

Silent authentication for Citrix Workspace

Citrix Workspace app introduces a Group Policy Object (GPO) policy to enable silent authentication for Citrix Workspace. This policy enables Citrix Workspace app to log in to Citrix Workspace automatically at system startup. Use this policy only when domain pass-through (single sign-on 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.

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.

Enabling authentication using conditional access

To enable authentication using conditional access with Azure AD, admins must perform the following steps:

1. Launch the registry editor.
2. Navigate to the following registry path:
   - For 64-bit operating systems: `Computer\HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\Citrix\Dazzle`
   - For 32-bit operating systems: `Computer\HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\Dazzle`
3. Create a registry value with the following attributes:

   Registry key name: EdgeChromiumEnabled

   Type: String Value

   Value: True
4. Restart the Citrix Workspace app for the changes to take effect.

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.

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)`
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)`

Scenario	Description	User-Agent
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

October 7, 2023

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.

> **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.

End Point Joined to	IdP	VDA Joined to	SSO to Citrix Workspace	SSO to VDA	Documentation
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 another IdP (AAD/Okta)	AD	Yes	Citrix Workspace app/FAS	Configure IdP using Configure 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.

End Point Joined to	IdP	VDA Joined to	SSO to Citrix Workspace	SSO to VDA	Documentation
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 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

End Point Joined to	IdP	VDA Joined to	SSO to Citrix Workspace	SSO to VDA	Documentation
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 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.

End Point Joined to	IdP	VDA Joined to	SSO to Citrix Workspace	SSO to VDA	Documentation
Non-Domain Joined	IdP that supports password less authentica-tion - 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.
- 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.

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	Domain pass-through authentica-tion

End Point Joined to	IdP	VDA Joined to	SSO to Citrix Workspace	SSO to VDA	Documentation
AD/Hybrid joined/Windows Hello for Business	StoreFront	AD	Yes(1)	Citrix Workspace app /FAS(2)	Domain pass-through authentication and Enable single sign-on for workspaces with Citrix Federated Authentication Service.
AD	Citrix Gateway - Advanced Authentication	AD	Yes	Citrix Workspace app(3))	
AD	Citrix Gateway - Basic authentication	AD	Yes	Citrix Workspace app(4)	Domain pass-through authentication.

Notes:

1. 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

October 7, 2023

> **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.

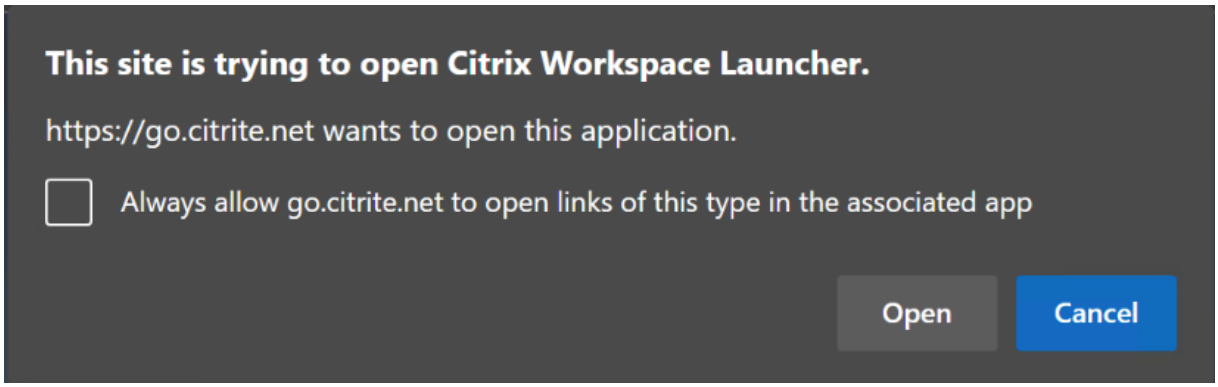
When launching StoreFront URL in a browser, the **Detect Receiver** prompt is shown.

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.

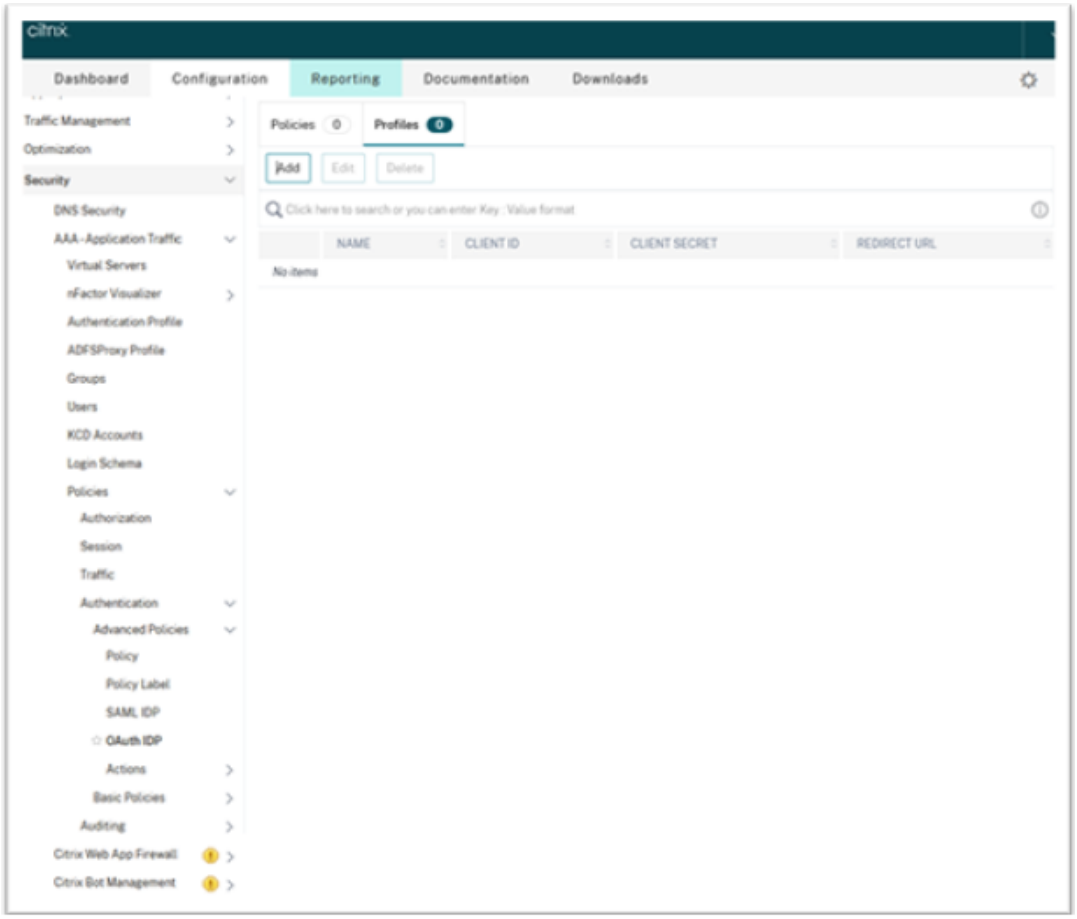
Create an OAuth IdP profile

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 <>

<!--NeedCopy-->
```

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.

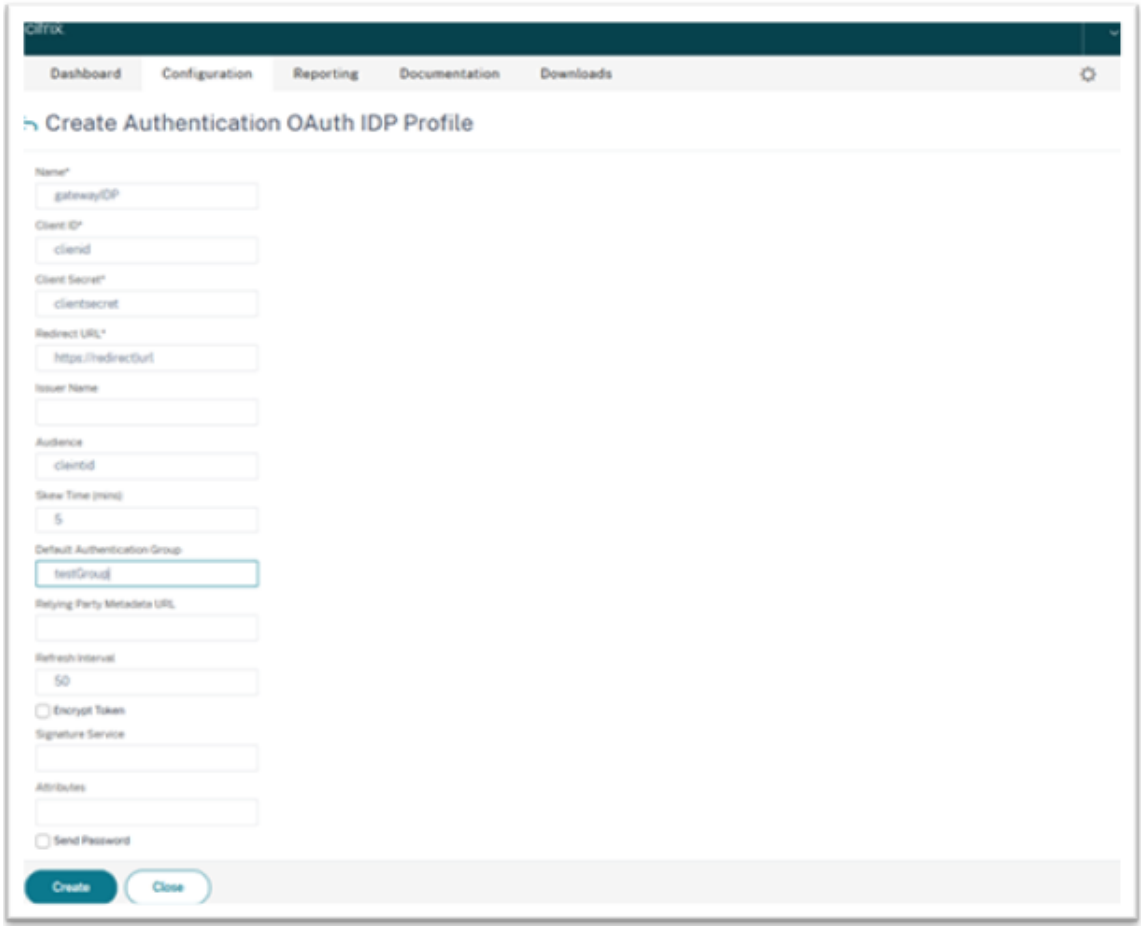
d) On the **Create Authentication OAuth IdP Profile** screen, set values for the following parameters and click **Create**.

- **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

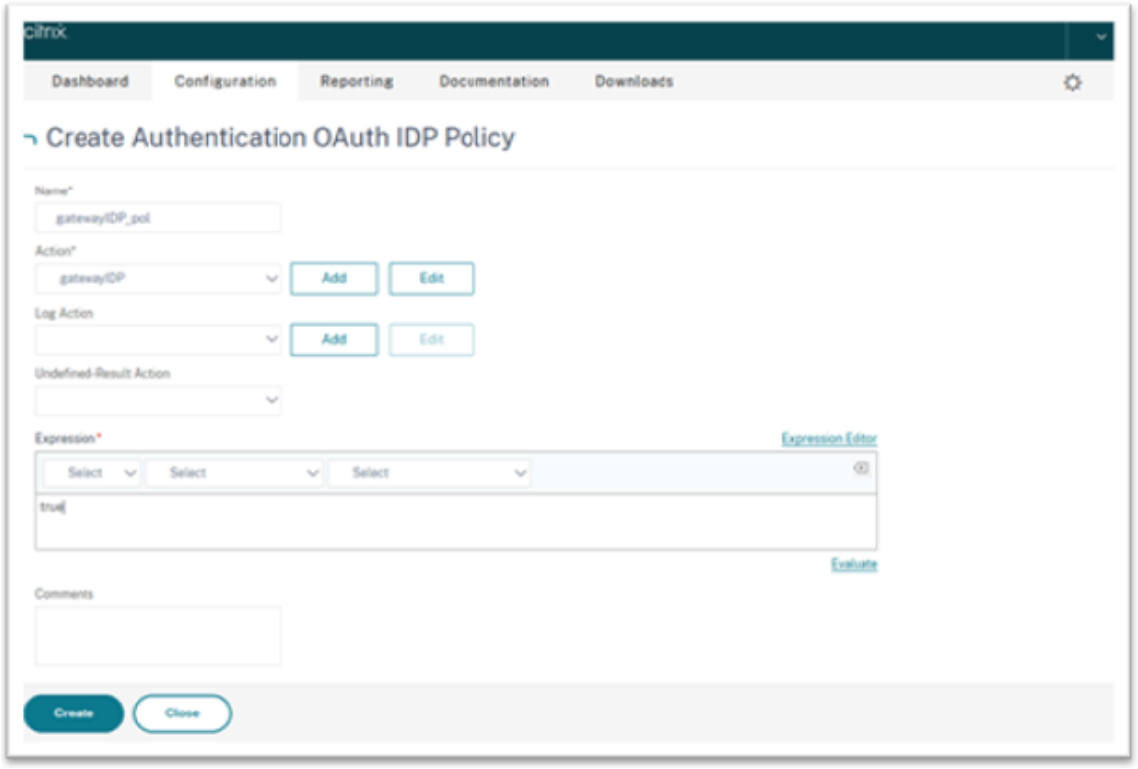
A group is added to the session for this profile to simplify policy evaluation and help in customizing policies. This group is the default group that is chosen when the authentication succeeds in addition to the extracted groups. Maximum Length: 63.



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**.

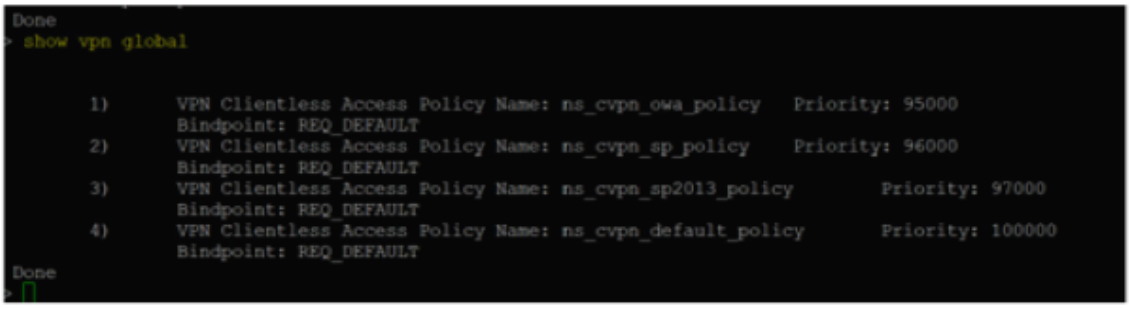
   - **Name** –Name of the LDAP Authentication Policy.
   - **Action Type** –Choose LDAP.
   - **Action** –Choose the LDAP action.
   - **Expression** –Default syntax expression that the policy uses to respond to specific request. For example, true**.

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:

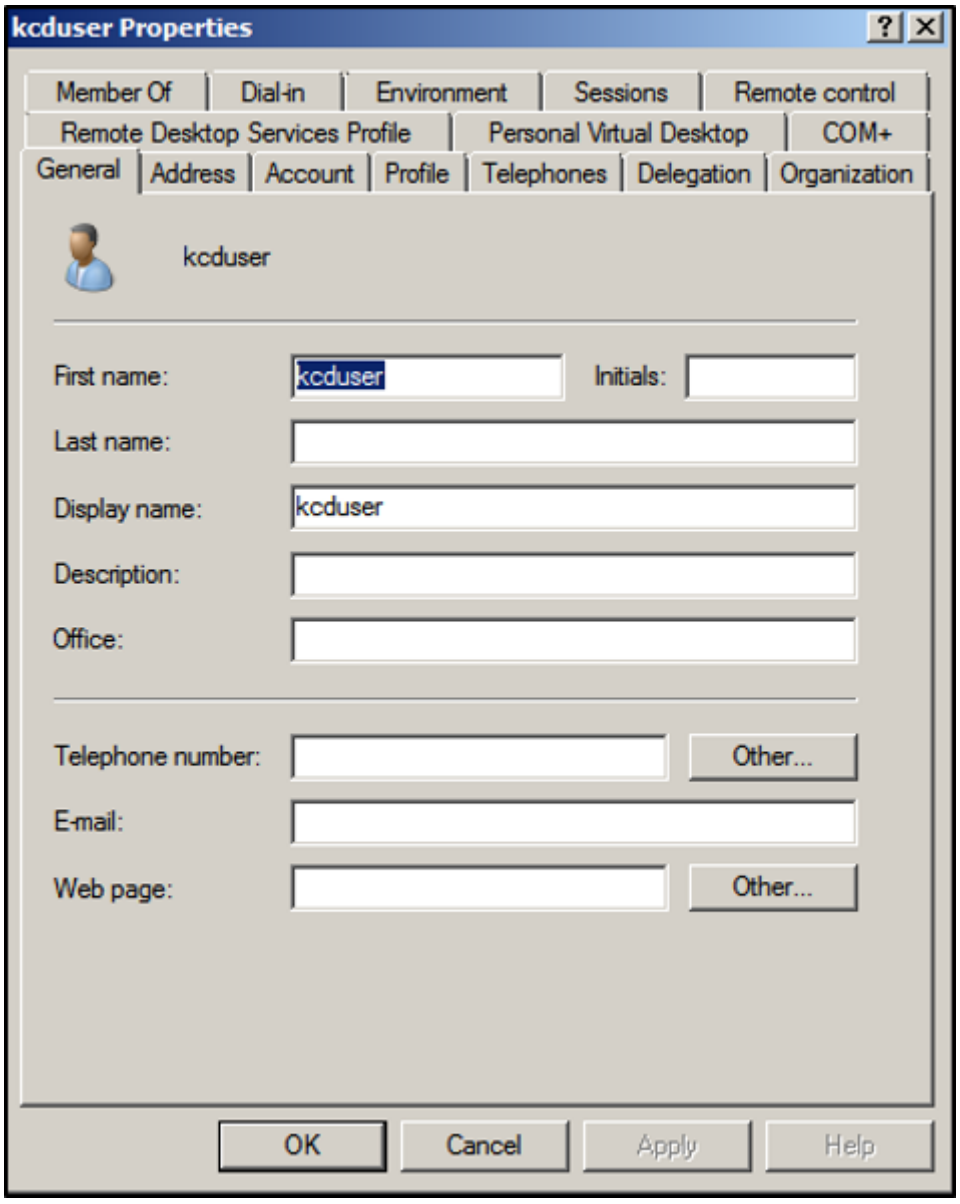
1. Kerberos Constrained Delegation configuration
2. Client configuration

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:

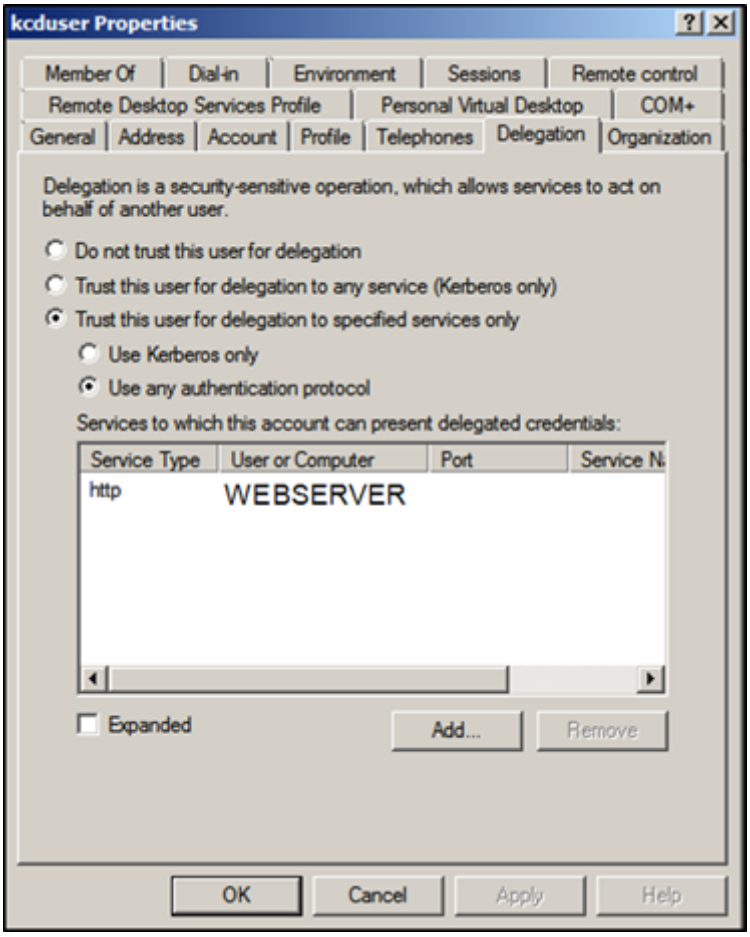
```
setspn –A http/<LB fqdn> <domain\Kerberos user>
```

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.

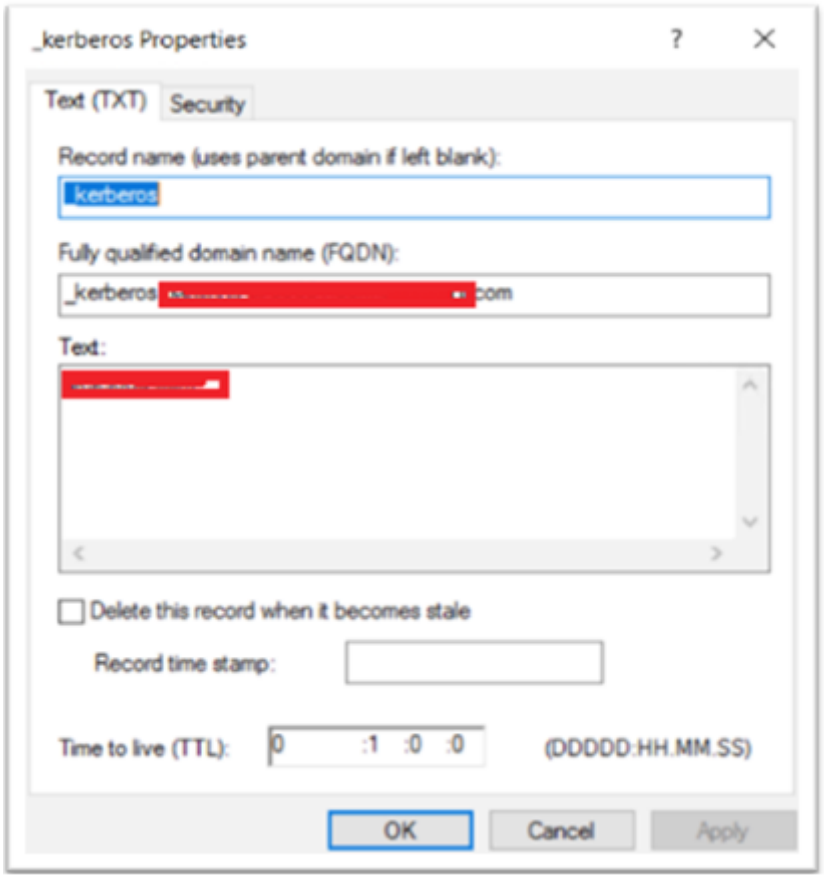


3. Create a DNS record for the client to find the Gateway's SPN:

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..



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:

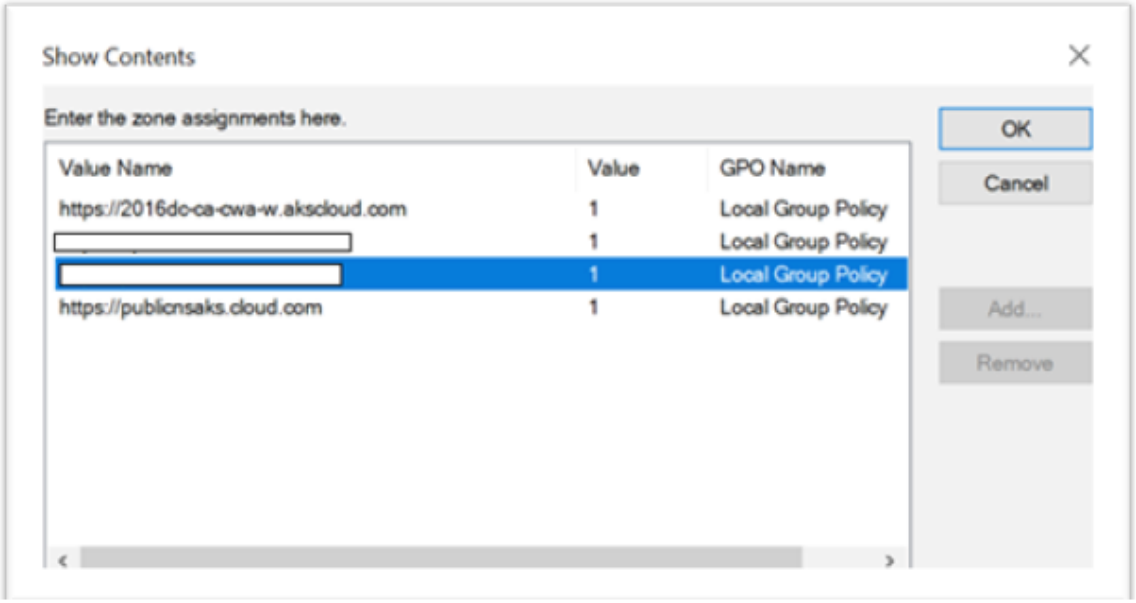
- Domain joined machine
- Citrix Workspace 2112.1or later with SSO setting enabled
- Trust necessary URLs that checks if the connections are secured
- Validate Kerberos from Client and AD. Client OS must have connectivity to AD to get Kerberos tickets.

Following are some of the URLs to be trusted in the browser:

- Gateway URL or FQDN
- AD FQDN
- Workspace 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

October 7, 2023

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.

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.

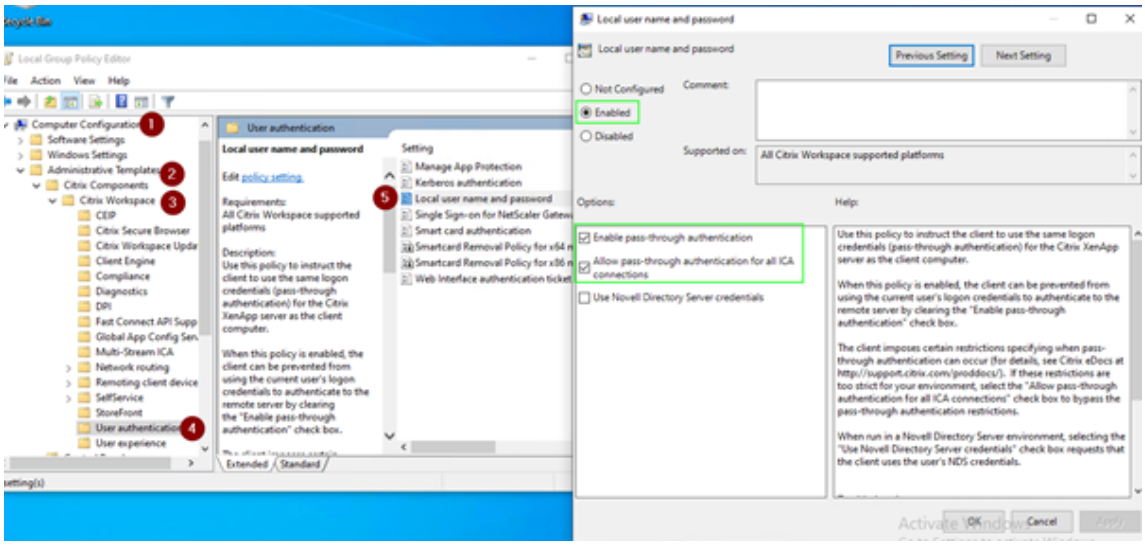
1. Install Citrix Workspace app from administrative command line with option `includeSSON`:

   ```
   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**.

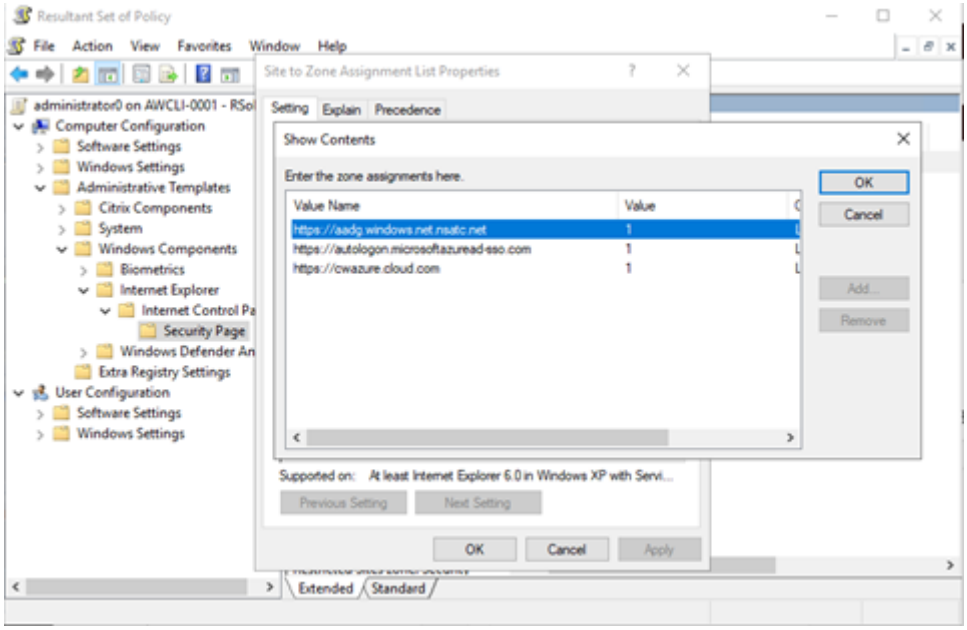
   > **Note:**
   >
   > These policies can be pushed to the client device via Active Directory. This step is required only when accessing Citrix Workspace from the web browser.

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`: Workspace URL

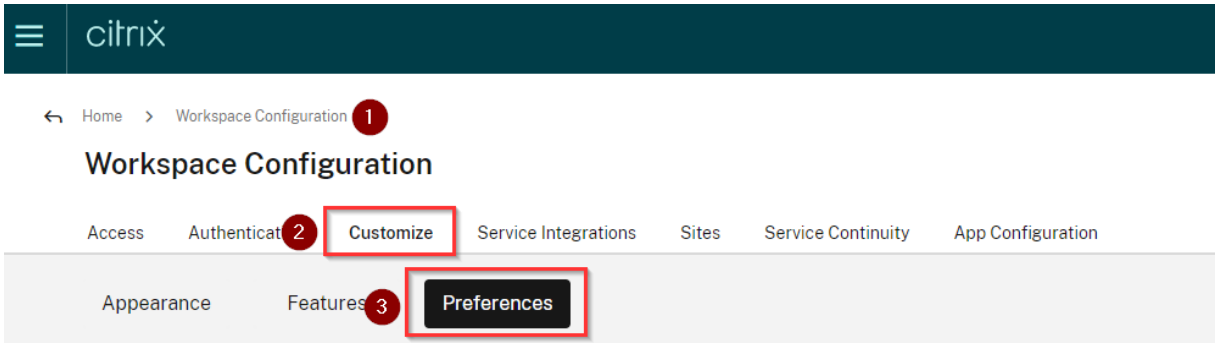


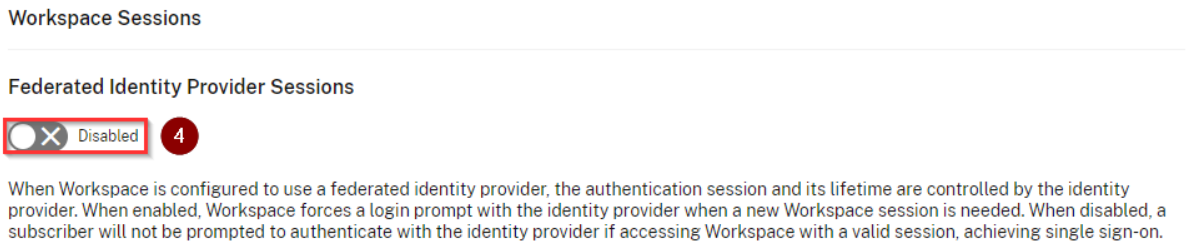
> **Note:**
>
> Single sign-on for AAD is disabled when the **AllowSSOForEdgeWebview** registry in `Computer\HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\Citrix\Dazzle` is set to false.

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 `Workspace Configuration\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:

  1. Select the **Change user sign-in** task and click **Next**.
  2. 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

October 7, 2023

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

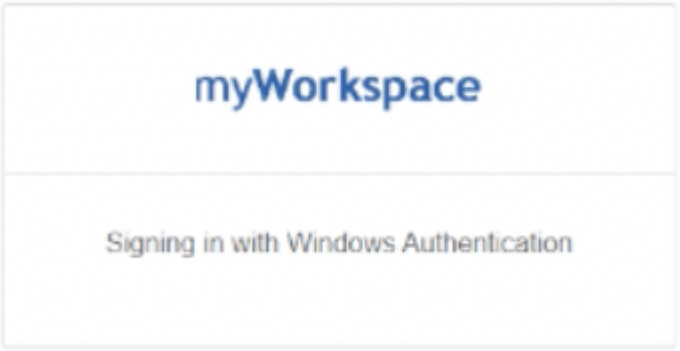
1. Deploy the Okta AD Agent:
   a) In the Okta Admin portal, click **Directory** > **Directory Integrations**.
   b) Click **Add Directory** > **Add Active Directory**.
   c) Review the installation requirements by following the workflow, which covers the Agent Architecture and Installation Requirements.
   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.

HDX

September 26, 2023

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

February 5, 2024

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:
  - **Citrix Virtual Desktops:** Configure the graphics memory limit using the **Citrix Machine Policy** setting Display memory limit.
  - **Citrix Virtual Apps:** Depending on the version of the Citrix Virtual Apps server, you've installed:
    - Configure the graphics memory limit using the **Citrix Computer Policy** setting Display memory limit.
    - From the Citrix management console for the Citrix Virtual Apps server, select the farm and in the task pane, select:
      - **Modify Server Properties** > **Modify all properties** > **Server Default** > **HDX Broadcast** > **Display** or

- **Modify Server Properties** > **Modify all properties** > **Server Default** > **ICA** > **Display**) and
  - Set the Maximum memory to use for each session's graphics.

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.

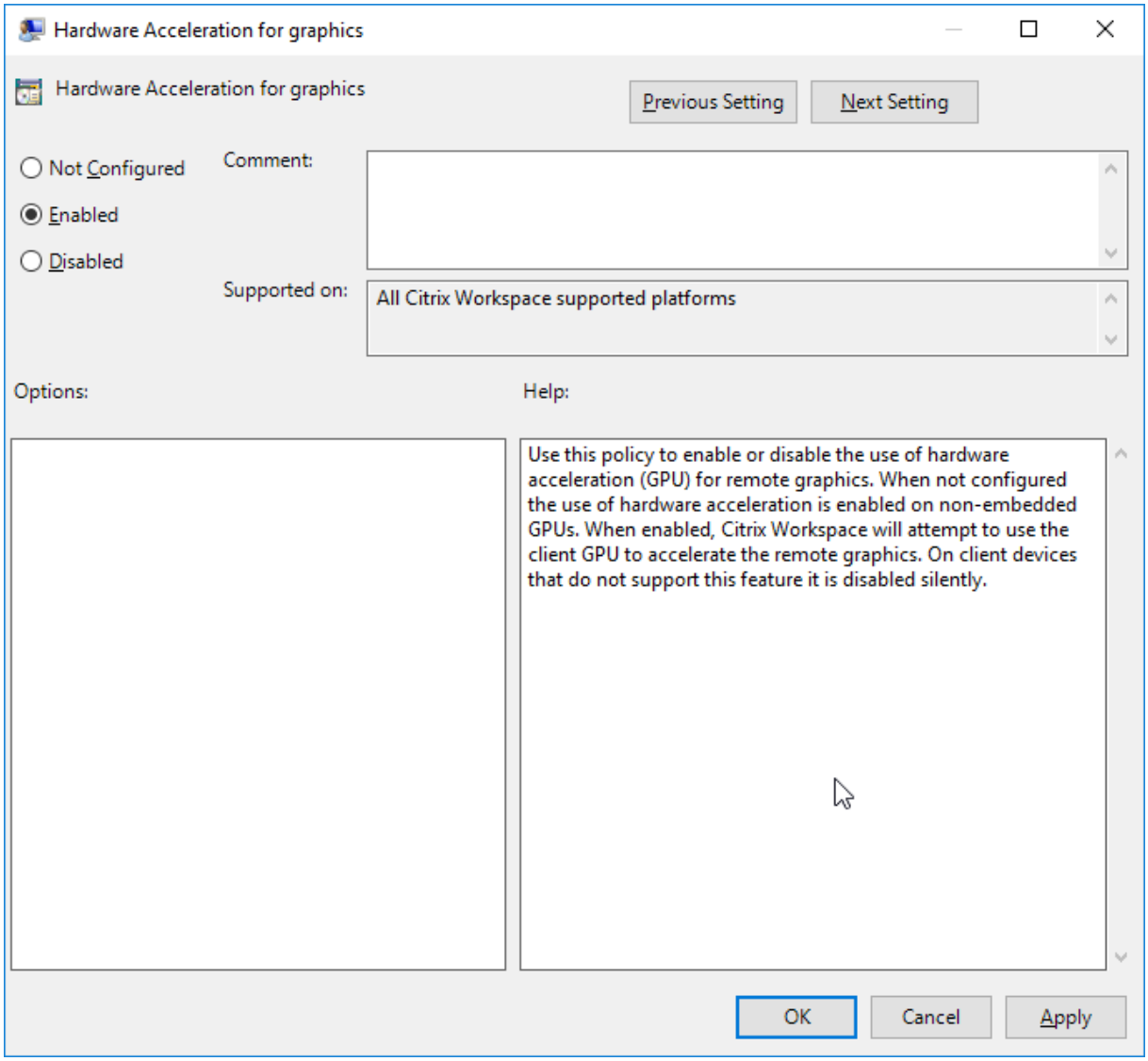
For calculating the session's graphic memory requirements for Citrix Virtual Apps and Desktops and Citrix DaaS, see Knowledge Center article CTX115637.

Hardware decoding

When using Citrix Workspace app (with HDX engine 14.4), the GPU can be used for H.264 decoding wherever it's available at the client. The API layer used for GPU decoding is DirectX Video Acceleration.

To enable hardware decoding using Citrix Workspace app Group Policy Object administrative template:

1. Open the Citrix Workspace app Group Policy Object administrative template by running gpedit.msc.
2. Under the **Computer Configuration** node, go to **Administrative Templates** > **Citrix Workspace** >**User Experience.**
3. Select **Hardware Acceleration for graphics**.
4. Select **Enabled** and click **Apply** and **OK**.



To validate if the policy is set and hardware acceleration is used for an active ICA session, check the following registry entries:

Registry Path: `HKEY_CURRENT_USER\SOFTWARE\Citrix\ICA Client\CEIP\Data\GfxRender`.

> **Tip**
>
> The value for **Graphics_GfxRender_Decoder** and **Graphics_GfxRender_Renderer** must be 2. If the value is 1, that means CPU-based decoding is being used.

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.

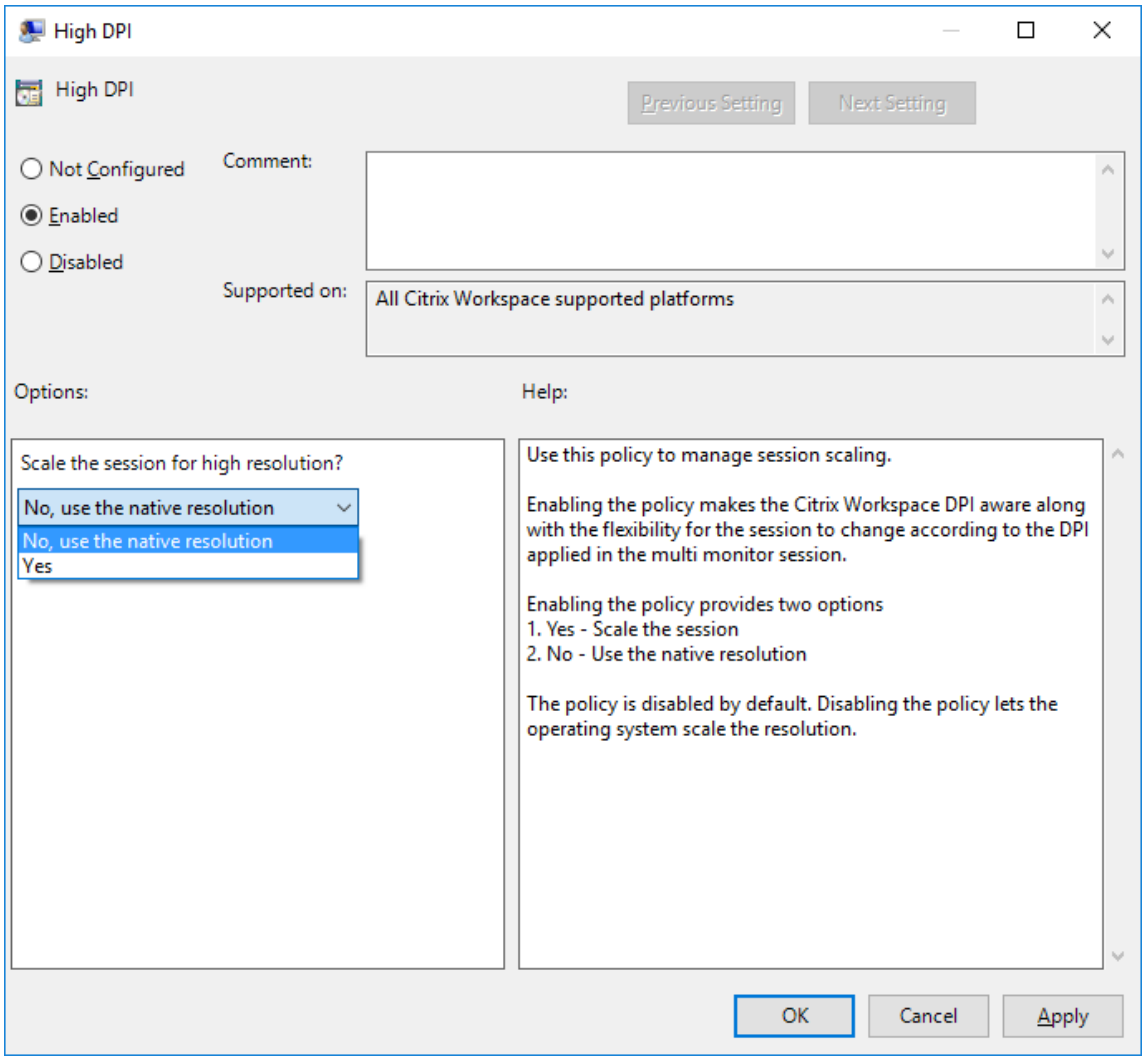
DPI scaling is mostly used with large size and high-resolution monitors to display applications, text, images, and other graphical elements in a size that can be viewed comfortably.

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 high DPI is applied in a session.

b) No, use the native resolution - Indicates that the resolution is set by the operating system.

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

Configure DPI scaling using the graphical user interface:

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 high DPI is applied in a session.
   b) **No, use the native resolution** - Indicates that the Citrix Workspace app detects the DPI on the VDA and applies it.
   c) **Let the operating system scale the resolution** - By default, this option is selected. It allows the Windows to handle the DPI scaling. This option also means that the High DPI policy is set to disabled.

4. Click **Save**.
5. Restart the Citrix Workspace app session for the changes to take effect.

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 default setting **Let the operating system scale the resolution** 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.

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. If the GPU on the endpoint doesn't support H.265 decoding using the DXVA interface, the H265 Decoding for graphics policy setting is ignored and the session falls back H.264 video codec.

Prerequisites:

1. VDA 7.16 and later.
2. Enable the **Optimize for 3D graphics workload** policy on the VDA.
3. Enable the **Use hardware encoding for video codec** policy on the VDA.

Client GPU that supports H.265 decoding:

- 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.

The use of H.265 can also be enabled by Configuring Citrix Workspace app to use H.265 video encoding using the Citrix Group Policy Object (GPO) administrative template:

1. Open the Citrix Workspace app Group Policy Object administrative template by running `gpedit.msc`.
2. Under the Computer Configuration node, go to **Administrative Templates > > User Experience**.
3. Select the H265 Decoding for graphics policy.
4. Select **Enabled**.
5. Click **Apply** and then **OK**.
6. Restart the session for the changes to take effect.

> **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.

Optimized Microsoft Teams

February 5, 2024

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.

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

February 5, 2024

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, adjusting the number of output buffers on the client as described in the Knowledge Center article CTX125027 has no effect.

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.

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

Browser content redirection

February 5, 2024

Browser content redirection prevents the rendering of webpages in the allow list on the VDA side. This feature uses Citrix Workspace app to instantiate a corresponding rendering engine on the client side, which fetches the HTTP and HTTPS content from the URL.

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

- Cookies are persistent across the sessions: When you exit and relaunch a browser, you aren't prompted to reenter your credentials.
- Browsers now honor the language set on the local system.

For more information, see Browser content redirection.

> **Note:**
>
> Browser Content Redirection supports only the Current Release of Citrix Workspace app for Windows. It doesn't support the Citrix Workspace app 1912 and 2203.1 LTSR versions.

To enable Browser Content Redirection on VDA, make sure the following policies on Citrix Web Studio are enabled:

- Browser Content Redirection
- Browser Content Redirection ACL Configuration
- Browser Content Redirection Authentication Sites

Configure path for Browser Content Redirection overlay Browser temp data storage

With the Citrix Workspace app 2303 version, you can configure the temp data storage path for the Chromium Embedded Framework (CEF) based browser. You can configure the path on VDA or client as follows:

On VDA:

1. Open the Registry Editor using `regedit` on the Run command.
2. Navigate to the `HKEY_LOCAL_MACHINE\Software\Citrix\DXMediaStream\ClientConfigurations\WindowsCef` registry path.
3. Create the string entry **BCRProfilePath** and set its value to folder for CEF based BCRtmp files. For example:

   ```
   "BCRProfilePath"="C:\\tmp\\AlternateBcrProfilePath"
   ```

4. Restart the session for the changes to take effect.

On client:

1. Open the Registry Editor using `regedit` on the Run command.
2. Navigate to the `HKEY_CURRENT_USER\Software\Citrix\HdxMediaStream` registry path.
3. Create a registry value with the following attributes:
   - Registry key name: `BCRProfilePath`
   - Registry value: string <`folder for CEF based BCRtmp files`>
4. Restart the Citrix Workspace app for the changes to take effect.

> **Note:**
>
> Starting with 2311.1 release, the version of the Chromium Embedded Framework (CEF) is upgraded to 117. This version upgrade helps to resolve security vulnerabilities.

Limitations:

Browser Content Redirection has the following limitations:

- Doesn't support Web Applications that require pop-up windows or session cookie persistence.
- Starting with Citrix Workspace app 2311.1 version, Microsoft Internet Explorer isn't supported.
- Applications that depend on the Google authentication service (For example, Google meet) are currently blocked.
- Extension plug-in isn't officially published on Microsoft Edge currently. However, there's a workaround to it.
- HTML5 video redirection policy must be disabled when Browser Content Redirection is in use.
- Sometimes, end users might be disconnected from their sessions because of unreliable networks, highly variable network latency, or range limitations of wireless devices. Browser Content Redirection doesn't have sufficient fallback or reporting mechanism for such scenarios.
- Files downloaded through the overlay are locally stored (on the end user's client machine).

Improved performance of BCR

Previously, BCR used client-side disk space cache and the cached information wasn't deleted during an upgrade. This setting resulted in higher disk space usage over time and inconsistent behavior while a page is redirected using BCR.

Starting with 2311.1 release, to resolve this issue, BCR uses an in-memory cache. This enhancement helps to improve the performance of BCR.

This feature is disabled by default. You can enable this feature on VDA or client as follows:

On VDA:

1. Open the Registry Editor using `regedit` on the Run command.
2. Navigate to the `HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\HDXMediaStream\ClientConfigurations\WindowsCef` registry path.
3. Create a `DWORD` key by the name `BCRStoreCEFCacheInMemory` and set the value of the key to 1.

If the value of `BCRStoreCEFCacheInMemory` is set to 0, BCR uses client disk space.

On client:

1. Open the Registry Editor using `regedit` on the Run command.
2. Navigate to the `HKEY_CURRENT_USER\Software\Citrix\HDXMediaStream` registry path.
3. Create a `DWORD` key by the name `BCRStoreCEFCacheInMemory` and set the value of the key to 1.

If the value of `BCRStoreCEFCacheInMemory` is set to 0, BCR uses client disk space.

> **Note:**
>
> - If the `BCRStoreCEFCacheInMemory` is set on both client and VDA, the setting on client takes precedence.
> - If both `BCRProfilePath` and `BCRStoreCEFCacheInMemory` are set, the configuration for `BCRProfilePath` takes precedence and the configuration for `BCRStoreCEFCacheInMemory` is ignored.

Limitation:

The in-memory cache size limit is set to 10MB.

Bidirectional content redirection

October 7, 2023

The bidirectional content redirection policy allows you to enable or disable client to host and host to client URL redirection. Server policies are set in Studio, and client policies are set from the Citrix Workspace app Group Policy Object administration template.

Citrix offers host to client redirection and Local App Access for client to URL redirection. However, we recommend that you use bidirectional content redirection for domain-joined Windows clients.

You can enable bidirectional content redirection using one of the following methods:

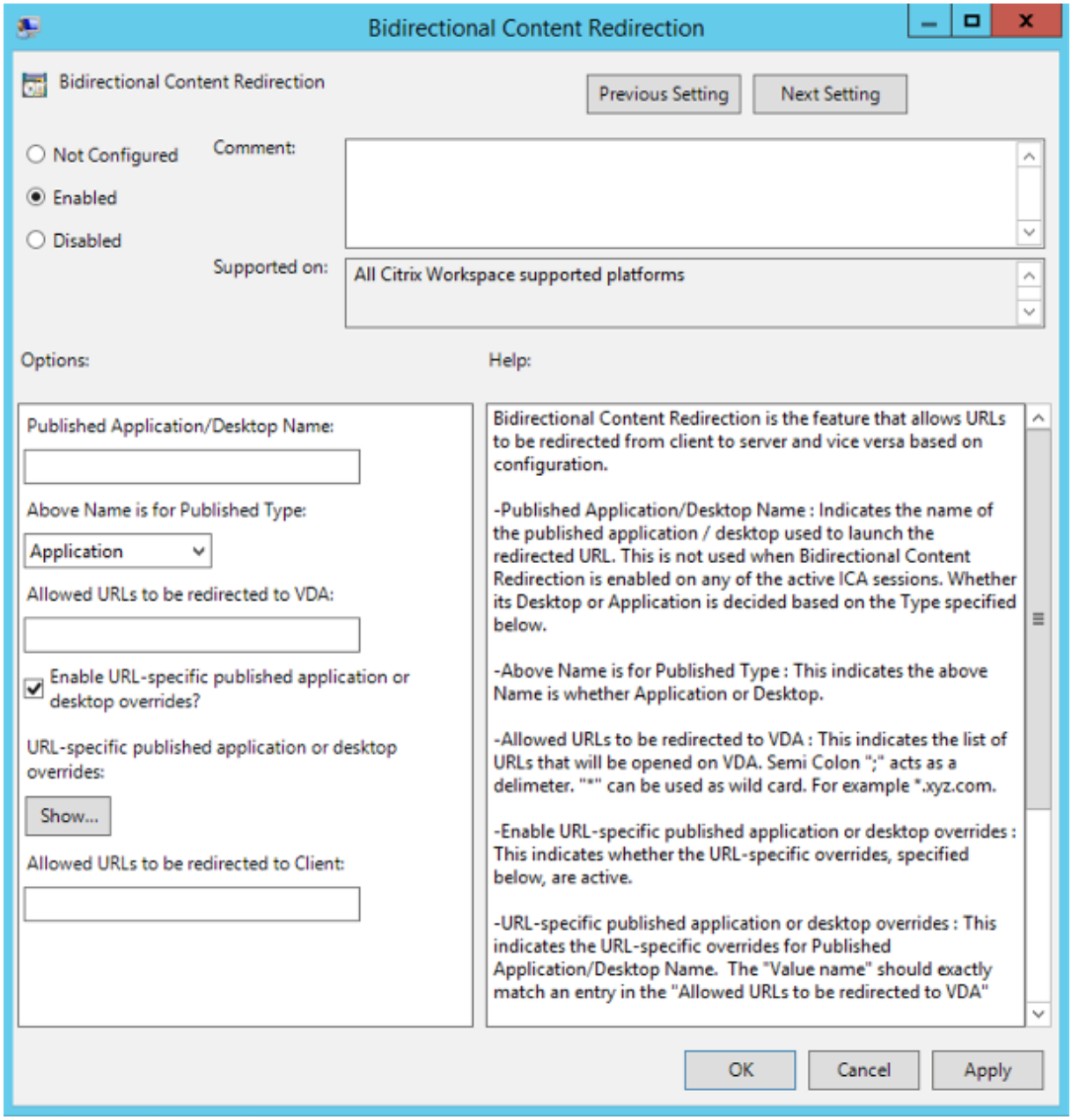
1. Group Policy Object (GPO) administrative template
2. Registry editor

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



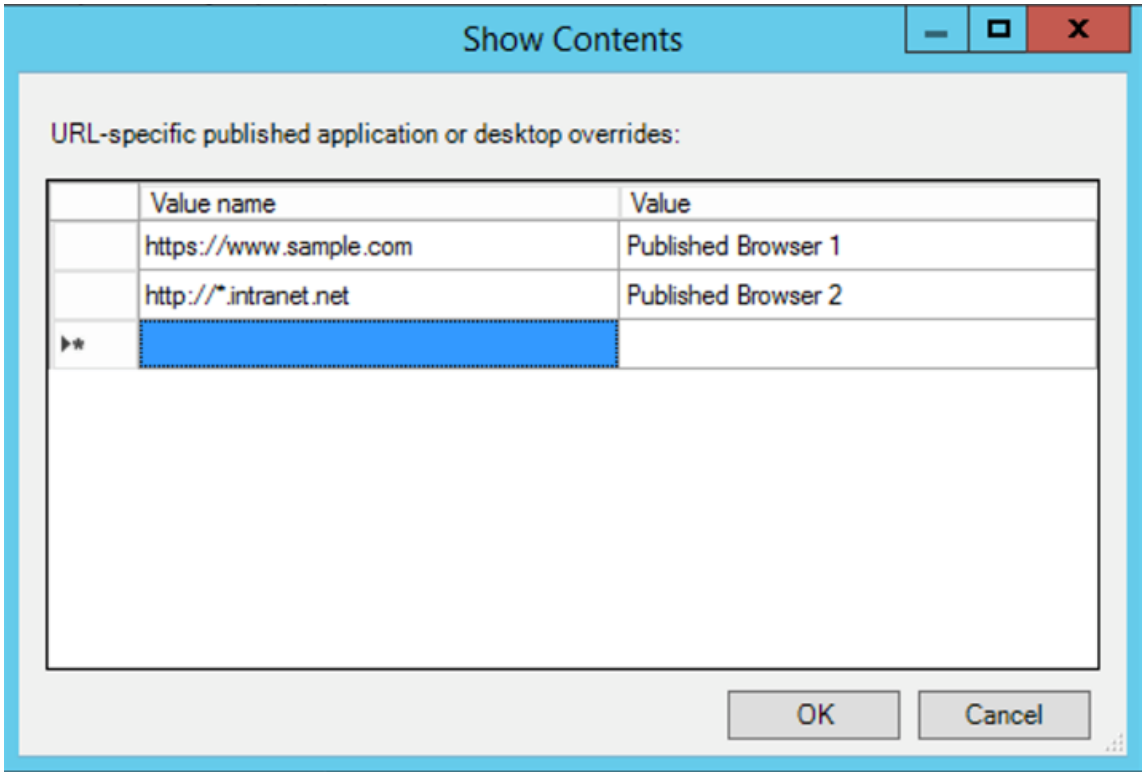
1. In the **Published Application or Desktop name** field, provide the name of the resource used to launch the redirected URL.

   > **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.

2. From the **Above Name is for Published Type**, select **Application** or **Desktop** of the resource as appropriate.
3. In the **Allowed URLs to be redirected to VDA** field, enter the URL that must be redirected. Sep-

arate the list with a semicolon.

4. Select the **Enable URL-specific published application for desktop overrides?** option to override a URL.
5. Click **Show** to display a list where the value name must match any of the URLs listed in the **Allowed URLs to be redirected to the VDA** field. The value must match a published application name.



6. In the **Allowed URLs to be redirected to Client:** field, enter the URL that must be redirected from the server to the client. Separate the list with a semicolon.

> **Note:**
>
> When you include URLs, specify a single URL or a semi-colon delimited list of URLs. You can use an asterisk (*) as a wildcard.

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

To enable bidirectional content redirection using the registry:

To enable bidirectional content redirection, run the `redirector.exe /RegIE` command on the Citrix Workspace app client and from the Citrix Workspace app installation folder `C:\Program Files (x86)\Citrix\ICA Client`.

Important:

- Ensure that the redirection rule does not result in a looping configuration. A looping configuration results if VDA rules are set so that, for example, a URL, `https://www.my\\_company.com` is configured to be redirected to the client, and the VDA.
- URL redirection supports only explicit URLs: URLs appearing in the address bar of the browser or found using the in-browser navigation, depending on the browser).
- If two applications with same display name use multiple StoreFront accounts, the display name in the primary StoreFront account is used for launching the application or a desktop session.
- New browser window opens only when a URL is redirected to the client. When a URL is redirected to VDA, if the browser is already open, then the redirected URL opens in the new tab.
- Embedded links in files like documents, emails, PDF is supported.
- Ensure that only one of the server file type associations exist and the host content redirection policies are set to Enabled on the same machine. Citrix recommends that you disable either the server file type association or the Host Content (URL) Redirection feature to confirm that URL redirection works properly.
- In Internet Explorer, click **Settings** > **Internet options** > **Advanced**, and select **Enable third-party browser extensions** check box under **Browsing** section.

Limitation:

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

Bi-directional URL support with Chromium-based browsers

Bidirectional content redirection allows you to configure URLs to redirect from client to server and from server to client using policies on the server and the client.

Server policies are set on the Delivery Controller and client policies on Citrix Workspace app. The policies are set using the Group Policy Object (GPO) administrative template.

Starting with Version 2106, bidirectional URL redirection support has been added for Google Chrome and Microsoft Edge.

Prerequisites:

- Citrix Virtual Apps and Desktops Version 2106 or later.
- Browser redirection extension version 5.0.

To register Google Chrome browser to bidirectional URL redirection, run the following command from the Citrix Workspace app installation folder:


```
%ProgramFiles(x86)%\Citrix\ICA Client\redirector.exe /regChrome /
verbose
```

> **Note:**
>
> When using these commands on Chrome browsers, the bidirectional content redirection extension installs automatically from the Chrome Web Store.

To unregister Google Chrome browser from bidirectional URL redirection, run the following command from the Citrix Workspace app installation folder:

```
%ProgramFiles(x86)%\Citrix\ICA Client\redirector.exe /unregChrome /
verbose
```

> **Note:**
>
> If you get the following error when accessing the Browser Extensions page, ignore the message:
>
> ```
> Websocket connection to wss://... failed.
> ```

For information on configuring URL redirection on Citrix Workspace app, see Bidirectional content redirection.

For more information about browser content redirection, see Browser content redirection in the Citrix Virtual Apps and Desktops documentation.

To prevent the desktop viewer window from dimming:

If you have multiple Desktop Viewer windows, by default the desktops that are not active are dimmed. If users want to view multiple desktops simultaneously, information on them might be unreadable. You can disable the default behavior and prevent the **Desktop Viewer** window from dimming by editing the Registry editor.

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

- On the user device, create a REG_DWORD entry called **DisableDimming** in one of the following keys, depending on whether you want to prevent dimming for the current user of the device or the device itself. An entry exists if the Desktop Viewer has been used on the device:
  - `HKEY_CURRENT_USER\Software\Citrix\XenDesktop\DesktopViewer`
  - `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\…

ICA Settings Reference

October 7, 2023

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

September 27, 2023

This section describes the following:

- Mouse
- Keyboard
- Printing
- USB
- Client drive-mapping
- Microphone

Mouse

October 7, 2023

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: RelativeMouse
- 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 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.

Keyboard

February 20, 2024

Keyboard shortcuts

You can configure combinations of keys that Citrix Workspace app interprets as having special functionality. When the keyboard shortcuts policy is enabled, you can specify Citrix Hotkey mappings, behavior of Windows hotkeys, and keyboard layout for sessions.

1. Open the Citrix Workspace app Group Policy Object administrative template by running gpedit.msc.

2. Under the **Computer Configuration node**, go to **Administrative Templates**> **Citrix Components** > **Citrix Workspace** > **User Experience**.
3. Select the Keyboard shortcuts policy.
4. Select **Enabled**, and the required options.
5. Restart the Citrix Workspace app session for the changes to take effect.

Citrix Workspace app support for 32-bit color icons:

Citrix Workspace app supports 32-bit high color icons. To provide for seamless applications, it automatically selects the color depth for:

- applications visible in the **Connection Center** dialog,
- the Start menu, and
- task bar

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

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.

Customizing location for application shortcut using the command line

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

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

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

Working with shortcuts

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

> **Note:**
>
> Windows 10 does not allow the creation of nested folders within the Start menu. Applications can appear under the root folder but not within the Category sub-folders that are defined with Citrix Virtual Apps.

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

Customizing location for application shortcut using the Registry editor

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

2. configure the registry keys, and then
3. reconfigure the store.

Manage workspace control reconnect

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

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

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

WSCReconnectMode key settings for Citrix Workspace app:

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

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

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

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

Name: **WSCReconnectModeUser**

Type: REG_SZ

Value data: `0`

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
```


Keyboard layout and language bar

Keyboard layout

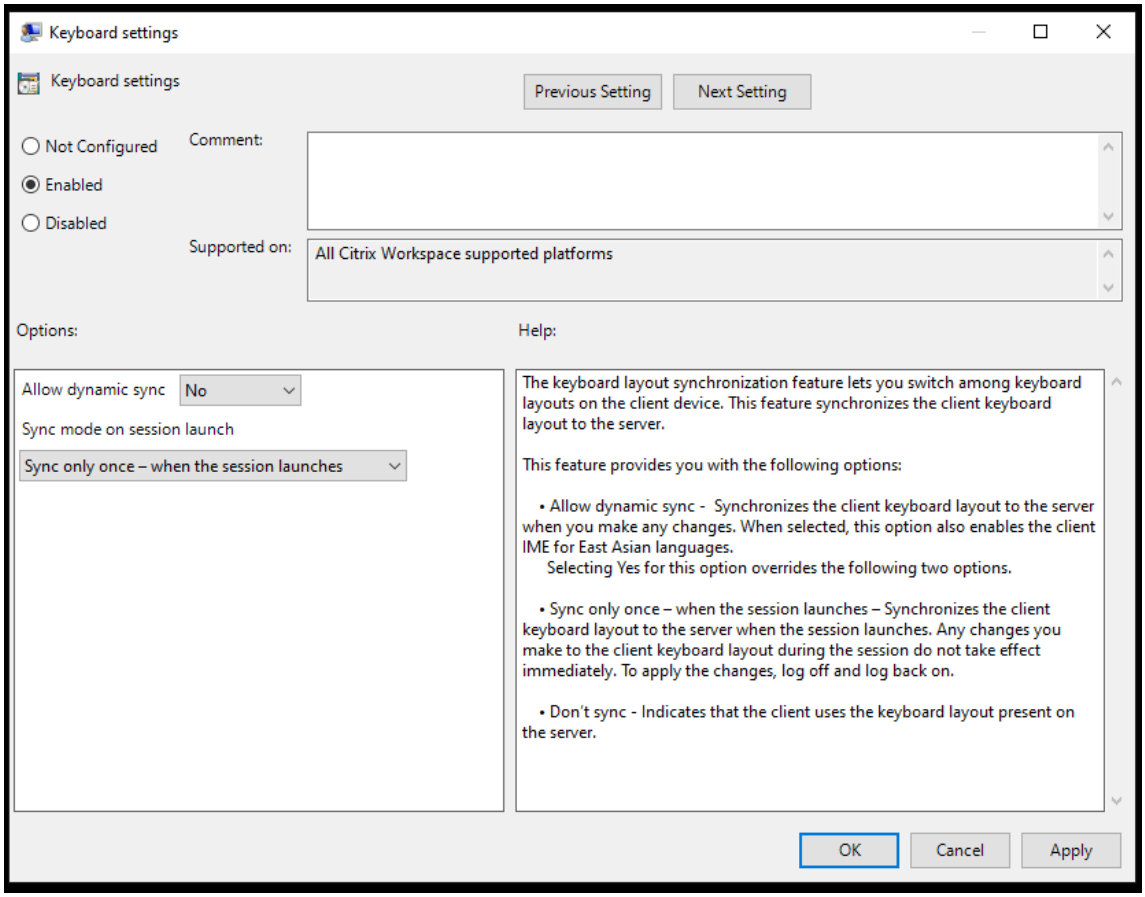
> **Note:**
>
> You can hide all or part of the Advanced Preferences sheet available from the Citrix Workspace app icon in the notification area. For more information, see Advanced Preferences sheet.

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:

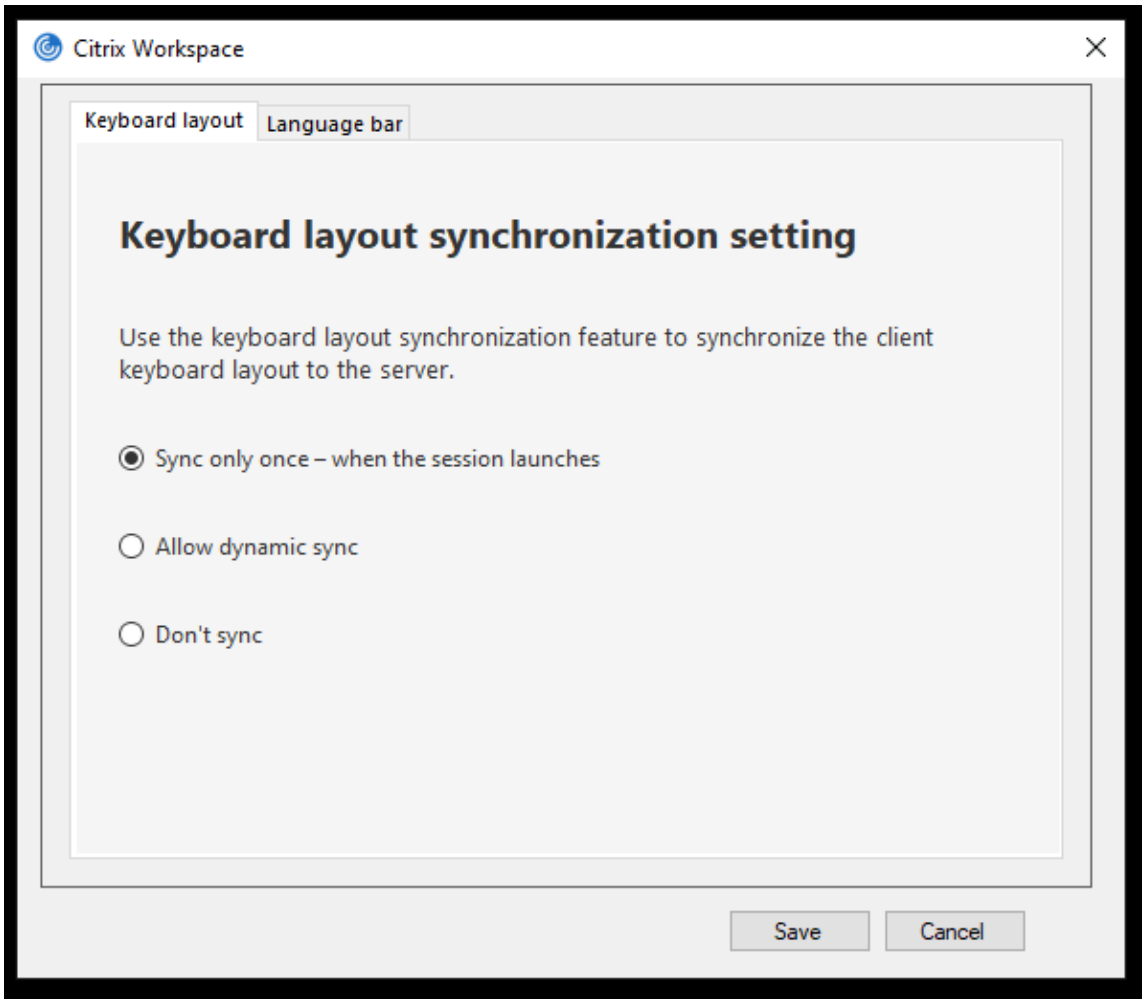
     – **Sync only once - when session launches** - Synchronizes the client keyboard layout to the server when the session launches. Any changes you make to the client keyboard layout during the session do not take effect immediately. To apply the changes, log off and log back on.
     – **Don't sync** - 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.

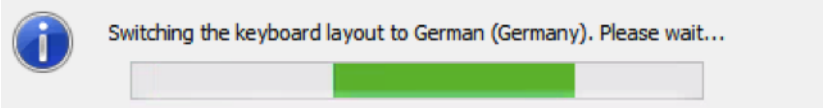
Typically, Citrix Workspace app installation folder is at C:\Program files (x86)\Citrix\ICA Client.

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**.

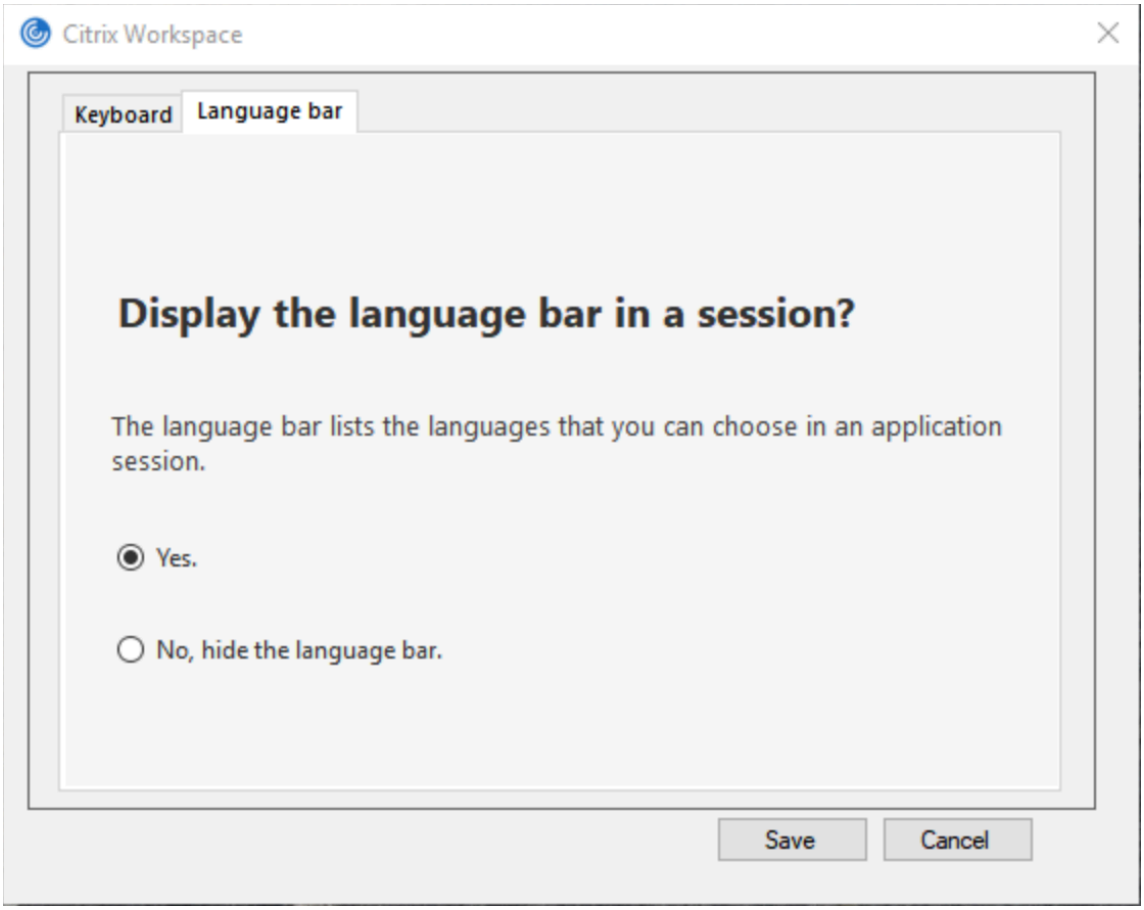
Configure language bar using the graphical user interface:

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.

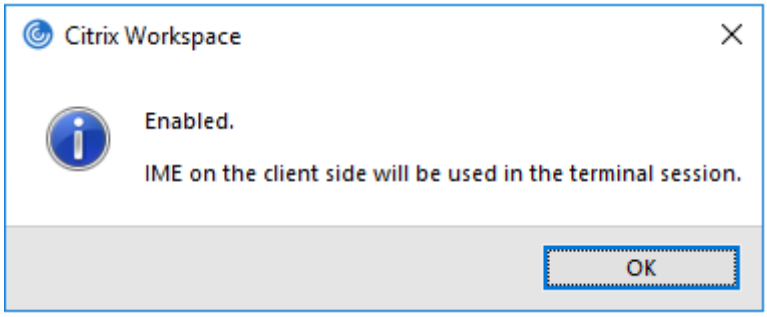
1. Launch the registry editor.
2. Navigate to `HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\ICA Client\Engine\Configuration\Advanced\Modules\LocalIME`.
3. Create a DWORD value key **ToggleOffLanguageBarFeature**, and set it to **1** to hide the Language bar option from the Advanced Preferences sheet.

Generic client Input Method Editors (IME)

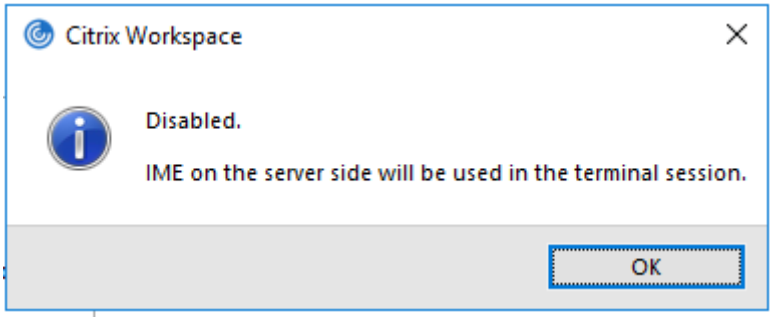
> **Note:**
>
> If you're using a Windows 10 Version 2004 operating system, you might face certain technical issues when using the IME feature in a session. Those issues are the result of a third-party limitation. For more information, see the Microsoft Support article.

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` .

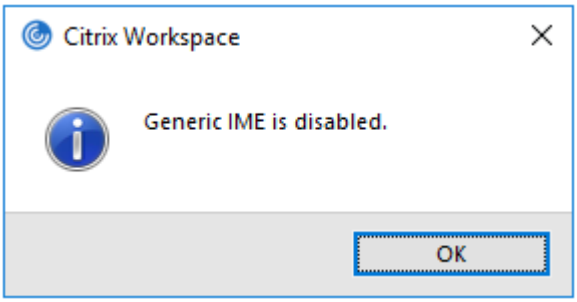


- To disable generic client IME, run the `wfica32.exe /localime:off` command from the Citrix Workspace app installation folder `C:\Program Files (x86)\Citrix\ICA Client`.

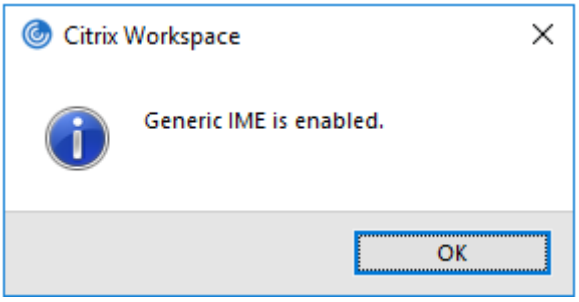


> **Note:**
>
> You can use the command-line switch `wfica32.exe /localime:on` to enable both generic client IME and keyboard layout synchronization.

- 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.

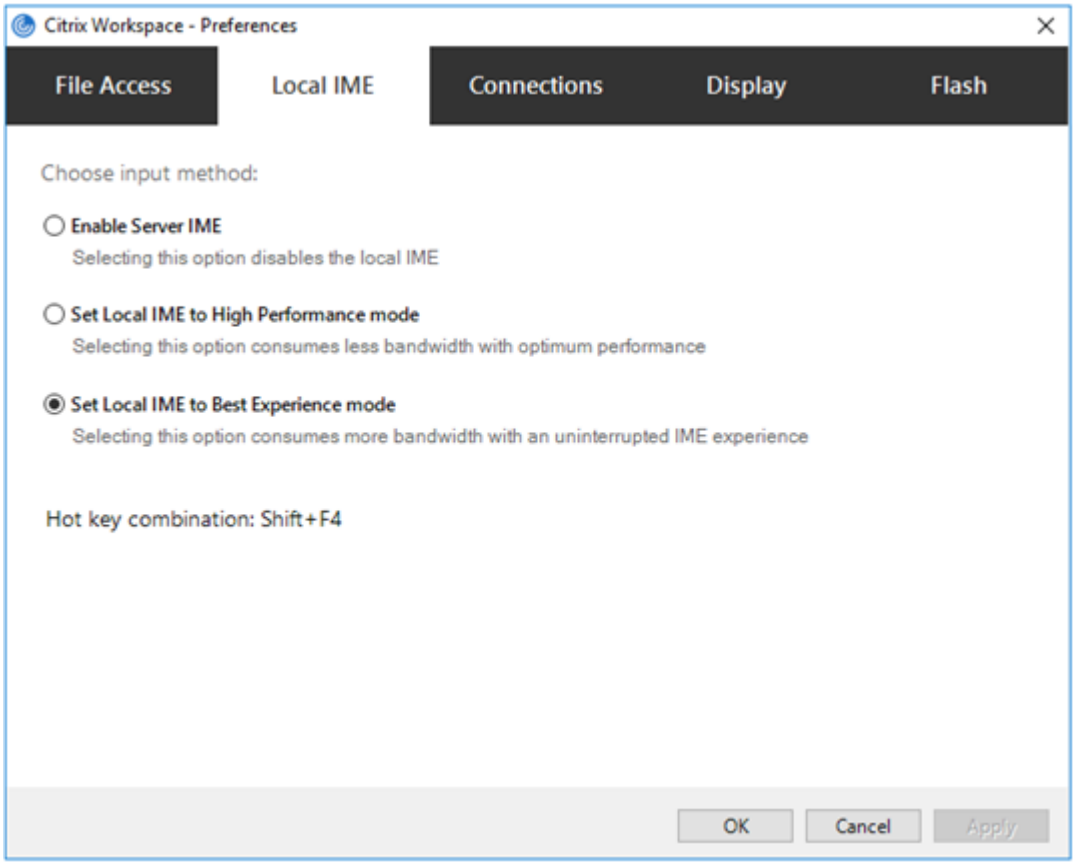
Configure generic client IME using the graphical user interface:

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 [Virtual Channels\Keyboard] 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

October 7, 2023

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 touch-screen devices in Citrix Virtual Apps and Desktops documentation.

On a touch-enabled client device, the Windows 10 VDA detects the presence of a keyboard or mouse when you connect or reconnect to a session. It also detects when you attach or detach a keyboard or mouse during the session. This feature is enabled by default on the VDA. To disable the feature, modify the **Tablet mode toggle** policy using Citrix Studio.

Tablet mode offers a user interface that is better suited to touchscreens:

- Slightly larger buttons.
- The **Start** screen and all the apps you start open in a full screen.
- The taskbar includes a Back button.
- Icons are removed from the taskbar.

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

> **Note:**
>
> Workspace for web doesn't support the Windows Continuum feature.

USB

October 7, 2023

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. For more information, see Knowledge Center article CTX123015.

- **Physical Interface Devices (Class 05)**- These devices are similar to Human Interface Devices (HIDs), but generally provide "real-time"input or feedback and include force feedback joysticks, motion platforms, and force feedback endoskeletons.
- **Still Imaging (Class 06)**- Includes digital cameras and scanners. Digital cameras often support the still imaging class which uses the Picture Transfer Protocol (PTP) or Media Transfer Protocol (MTP) to transfer images to a computer or other peripheral. Cameras 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. For instructions, see Knowledge Center article CTX123015.

- **Mass Storage (Class 08)**- The most common mass storage devices are USB flash drives; others include USB-attached hard drives, CD/DVD drives, and SD/MMC card readers. There are a wide variety of devices with internal storage that also present a mass storage interface; these include media players, digital cameras, and mobile phones. Mass Storage (Class 08) is not applicable to 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. For instruction, see Knowledge Center article CTX123015.

- **Personal Healthcare (Class 0f)**- These devices include personal healthcare devices such as blood pressure sensors, heart rate monitors, pedometers, pill monitors, and spirometry.
- **Application and Vendor Specific (Classes fe and ff)**- Many devices use vendor-specific 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 make changes to 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 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:

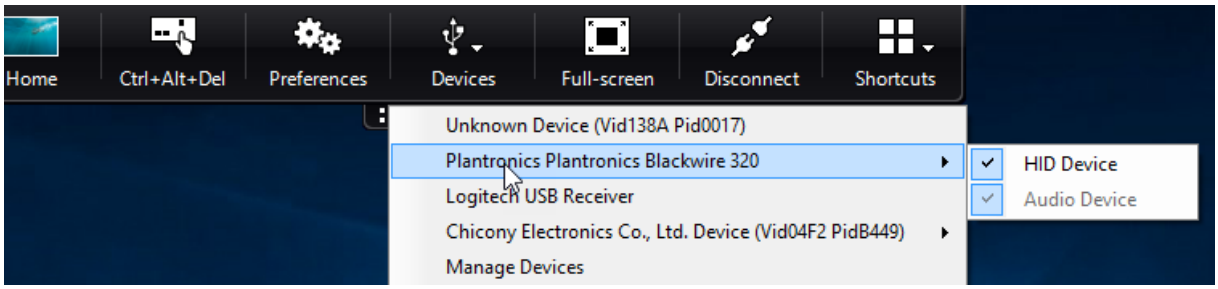
1. Open the Citrix Workspace app Group Policy Object administrative template by running gpedit.msc.
2. Under the **User Configuration** node, go to **Administrative Templates** > **Citrix Components** > **Citrix Workspace** > **Remoting client devices** > **Generic USB Remoting**.
3. Select the **USB 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.

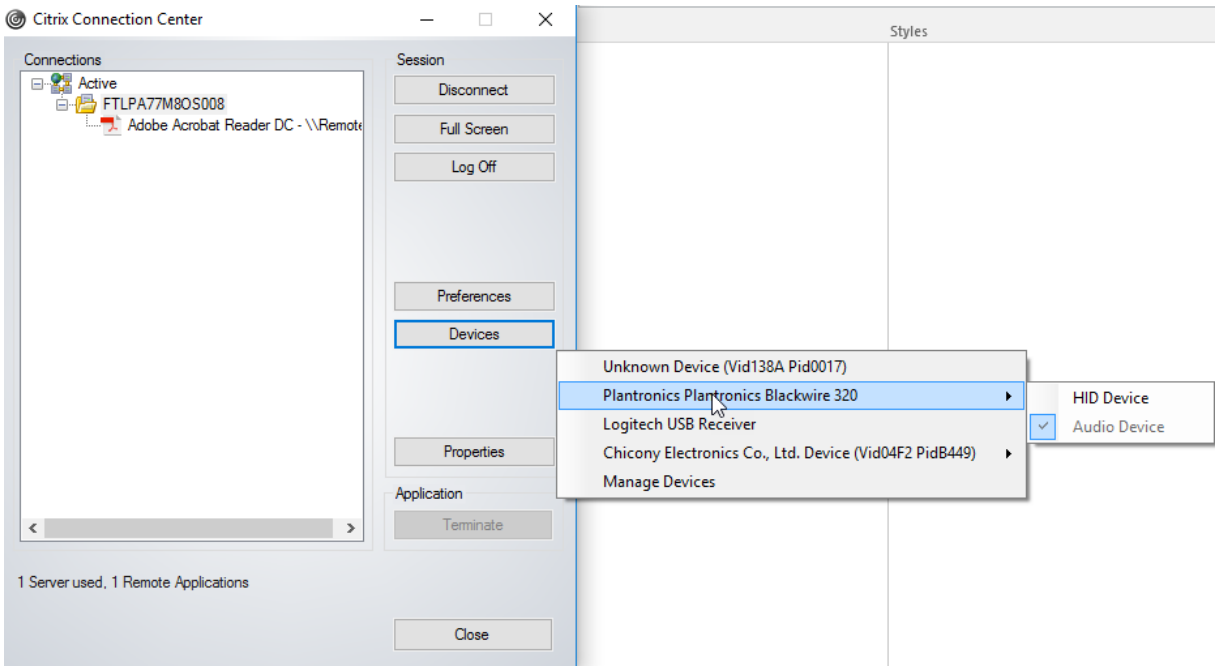
Connecting USB devices:

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:

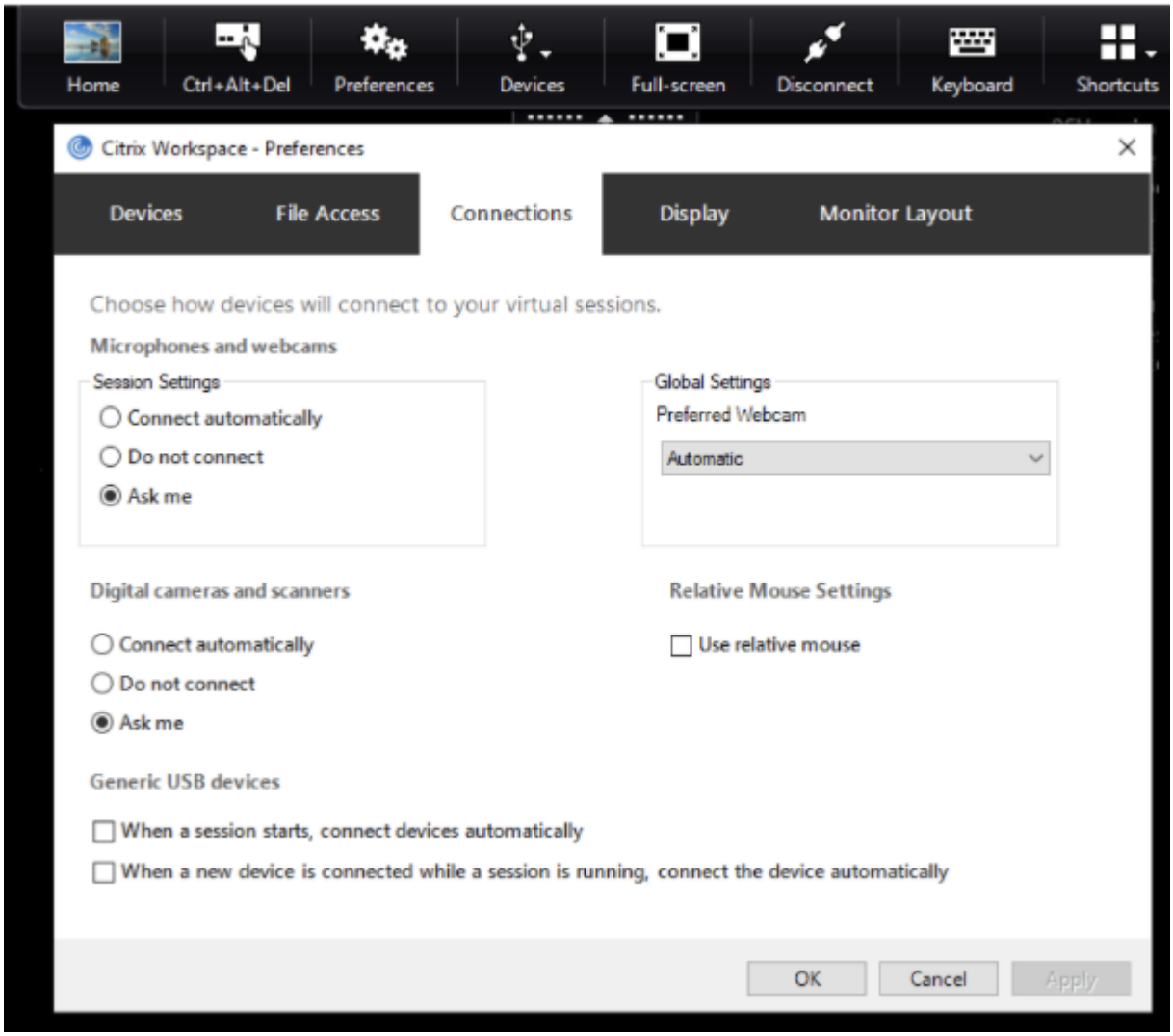
The CONNECT keyword introduced in Citrix Workspace app for Windows 2109 allows for automatic redirection of USB devices. The CONNECT rule can replace the ALLOW rule if the administrator allows the device or selected interfaces to automatically connect in the session.

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.

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 allows 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 **Split-Devices** policy. However, you must use the Bloomberg keyboard feature instead of this policy for the Bloomberg keyboard 4.

The support for the Bloomberg keyboard changes the way certain USB devices are redirected to a session. This support is not enabled by default.

- To enable the support during the installation time, specify the value of the **ENABLE_HID_REDIRECTION** property as TRUE at the installation command-line. For example:

```
CitrixOnlinePluginFull.exe /silent
ADDLOCAL="ICA_CLIENT,PN_AGENT,SSON,USB"
ENABLE_SSON="no"INSTALLDIR="c:\test"
ENABLE_DYNAMIC_CLIENT_NAME="Yes"
DEFAULT_NDSCONTEXT="Context1,Context2"
SERVER_LOCATION="http://testserver.net"ENABLE_HID_REDIRECTION="
TRUE"
```

- To enable support after installing the online plug-in, edit the Windows Registry on the system where the online plug-in is running:

  1. Open Registry Editor.
  2. Navigate to the following key: `HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\ICA Client\GenericUSB`
  3. If the value **EnableBloombergHID** exists, modify it so that the value data is 1.
  4. If the value **EnableBloombergHID** does not exist, create a DWORD value with the name EnableBloombergHID and provide the value data as 1.

Disabling support for the Bloomberg keyboard:

You can disable support for the Bloomberg keyboard in the online plug-in as follows:

1. Open Registry Editor on the system running the online plug-in software.
2. Navigate to the following key: `HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\ICA Client\GenericUSB`

3. If the value **EnableBloombergHID** exists, modify it so that the value data is 0 (zero).

   If the value **EnableBloombergHID** doesn't exist, it indicates that the support for the Bloomberg keyboard is not enabled. In such 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.

Client drive-mapping

October 7, 2023

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

October 7, 2023

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

October 7, 2023

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').

> **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 are typically found in the `C:\Program Files\Citrix\ICA Client\Configuration` directory.

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

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

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

> **Note:**
>
> - If the CitrixBase.admx\adml isn't added to the local GPO, the **Enable ICA File Signing** policy might be lost.

- When upgrading Citrix Workspace app, add the latest template files to local GPO. Earlier settings are retained after import. For more information, see the following procedure:

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

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

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

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

Note:

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

Session experience

February 9, 2024

Application launch time

Use the session prelaunch feature to reduce application launch time during normal or high traffic periods, thus providing users with a better experience. The prelaunch feature allows to create a prelaunch session. Prelaunch session is created when a user logs on to Citrix Workspace app, or at a scheduled time if the user has signed in.

The prelaunch session reduces the launch time of the first application. When a user adds 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_DWORD

Values:

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

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

Name: **State**
Type: REG_DWORD

Values:

0 - Disable prelaunch.

1 - Enable just-in-time prelaunch. (prelaunch starts after the user's credentials are authenticated.)

2 - Enable scheduled prelaunch. (prelaunch starts at the time configured for Schedule.)

Name: **Schedule**
Type: REG_DWORD

Value:

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

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 is directed to the local computer.

Key presses that activate certain Microsoft accessibility features, for example, Sticky Keys, Filter Keys, and Toggle Keys are normally directed to the local computer.

As an accessibility feature of the Desktop Viewer, pressing Ctrl+Alt+Break displays the **Desktop Viewer** toolbar buttons in a pop-up window.

Ctrl+Esc is sent to the remote, virtual desktop.

> **Note:**
>
> By default, if the Desktop Viewer is maximized, Alt+Tab switches focus between windows inside the session. If the Desktop Viewer is displayed in a window, Alt+Tab switches focus between windows outside the session.

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.

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.

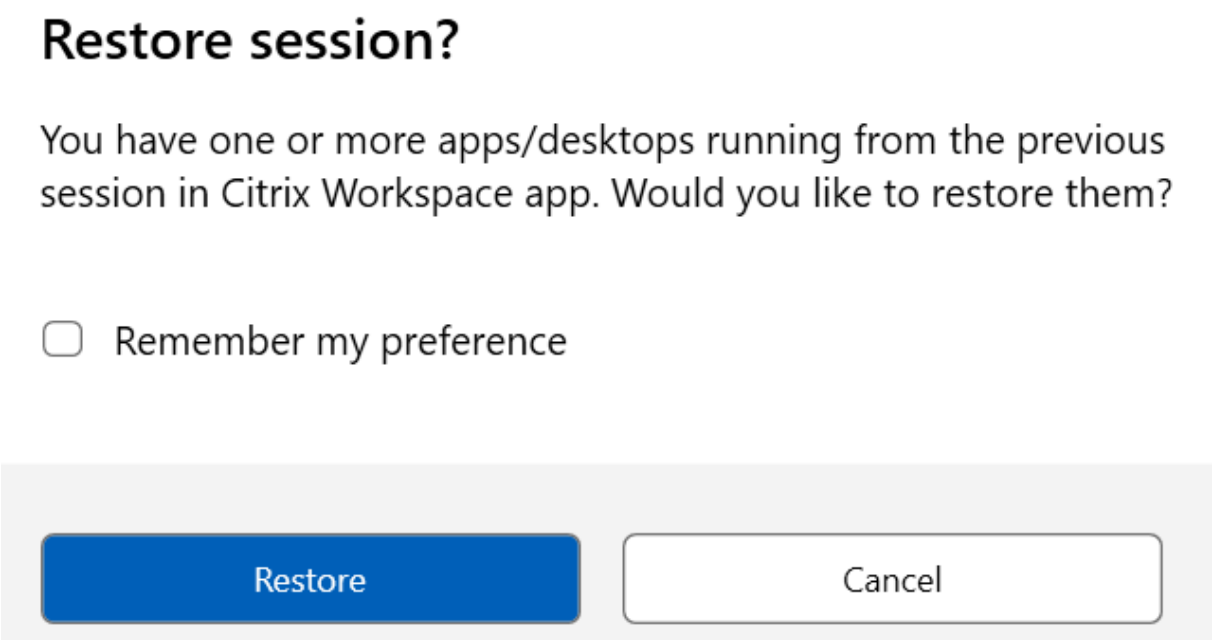
When you configure this key, the status indicator might appear and disappear frequently. This behavior is as designed. To suppress the status indicator, do the following:

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)

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:



This prompt appears only when the **show reconnection prompt to reconnect sessions** is set to true in the Global App Configuration service.

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.

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.

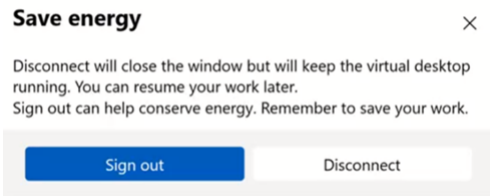
Sustainability initiative from Citrix Workspace app

For native launch

From Citrix Workspace app 2309 version onwards, 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 shutdown 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 `LogoffOnClose` keyword to **true** in the **Description** field.
9. Click **OK**. The following dialog box appears when you close the virtual desktop:

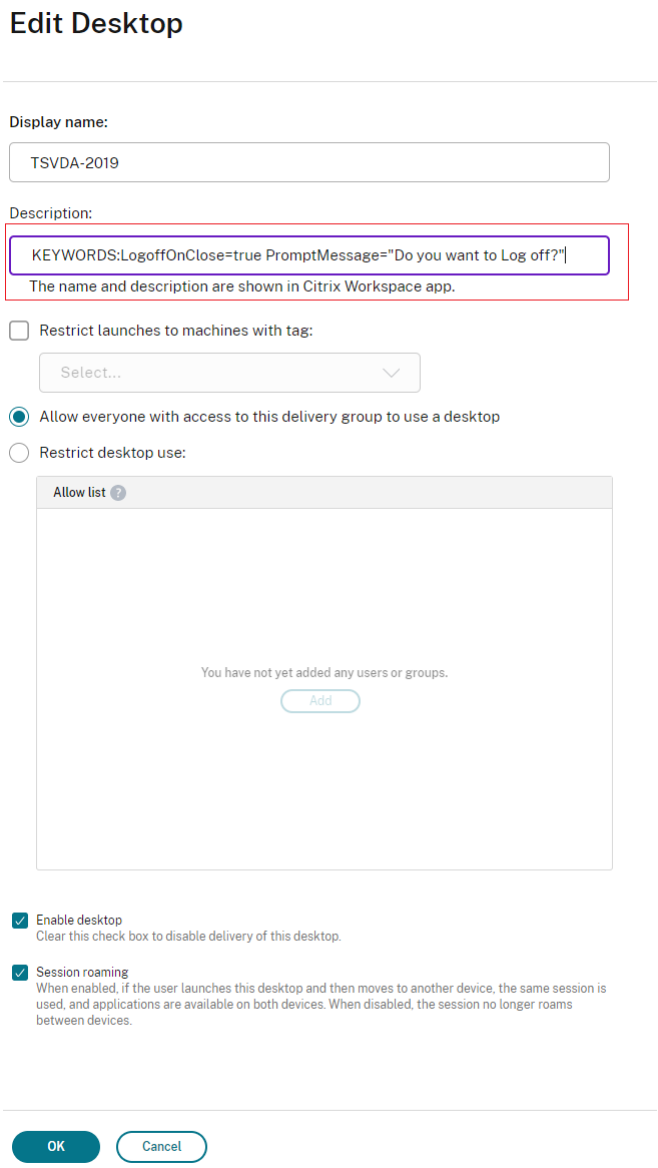


Customizing the text in the Save energy screen You can also customize the text in the **Save energy** screen.

1. Follow steps 1–8 in the preceding section.
2. Set the `PromptMessage` keyword to the required text in the **Description** field.

   Example:

```
KEYWORDS:LogoffOnClose=true PromptMessage="Do you want to Log off?
    "
<!--NeedCopy-->
```



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
<!--NeedCopy-->
```

With this PowerShell script, it is 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 unique description value and possible set of different keywords.

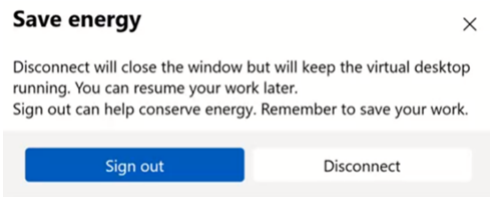
3. Click **OK**. The following dialog box appears when you close the virtual desktop.

For hybrid cloud launch

From Citrix Workspace app 2402 version, this feature is available for hybrid launches on cloud. Once this feature is enabled, a prompt is displayed 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 shutdown 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.

   > **Note:**
   >
   > The maximum number of characters allowed in the Description field is 200.

   Example:

   ```
   KEYWORDS:ICA-LogOffOnClose=true ="Do you want to Log off?"
   <!--NeedCopy-->
   ```

   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
   <!--NeedCopy-->
   ```

   With this PowerShell script, it is 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 unique description value and possible set of different keywords.

3. Click **OK**. The following dialog box appears when you close the virtual desktop.

Citrix Workspace app Desktop Lock

October 7, 2023

You can use the Citrix Workspace app Desktop Lock when you do not need to interact with the local desktop. You can use the Desktop Viewer (if enabled), however it has only the following set of options on the toolbar:

- Ctrl+Alt+Del
- Preferences
- Devices
- Disconnect.

Citrix Workspace app for Windows with Desktop Lock works on domain-joined machines that are single sign-on enabled and store configured. It doesn't support PNA sites. Previous versions of Desktop Lock aren't supported when you upgrade to Citrix Receiver for Windows 4.2 or later.

> **Note:**
>
> When using Citrix Workspace app for Windows with Desktop Lock, a user is signed in to the first desktop that is alphabetically sorted with the name of all the desktops that are available to the user. Currently, there is no option to selectively choose which desktop the user must sign in. Also, this feature supports only desktops and doesn't support apps.

Install Citrix Workspace app for Windows with the `/includeSSON` flag. Configure the store and single sign-on, either using the adm/admx file or command line option. For more information, see Install.

Then, install the Citrix Workspace app Desktop Lock as an administrator using the `CitrixWorkspaceDesktopL` `.msi` available in the Citrix Downloads page.

System requirements

- Microsoft Visual C++ 2005 Service Pack 1 Redistributable Package. For more information, see the Microsoft Download page.

- Supported on Windows 10 (Anniversary update included), and Windows 11.
- Connects to StoreFront through native protocols only.
- Domain-joined end points.
- User devices must be connected to a LAN or WAN.

Local App Access

> **Important**
>
> Enabling Local App Access might allow local desktop access unless a full lockdown has been applied with the Group Policy Object template or a similar policy. For more information, see the Configure Local App Access and URL redirection section in the Citrix Virtual Apps and Desktops documentation.

Working with Citrix Workspace app Desktop Lock

- You can use Citrix Workspace app Desktop Lock with the following Citrix Workspace app features:
  - 3Dpro, Flash, USB, HDX Insight, Microsoft Lync 2013 plug-in, and Local App Access
  - Domain, two-factor authentication, or smart card authentication only
- Disconnecting the Citrix Workspace app Desktop Lock session logs out the end device.
- Flash redirection is disabled on Windows 8 and later versions. Flash redirection is enabled on Windows 7.
- The Desktop Viewer is optimized for Citrix Workspace app Desktop Lock with no Home, Restore, Maximize, and Display properties.
- Ctrl+Alt+Del is available on the Desktop Viewer toolbar.
- Most windows shortcut keys are passed to the remote session, except for Windows+L.
- Ctrl+F1 triggers Ctrl+Alt+Del when you disable the connection or Desktop Viewer for desktop connections.
- A local user profile is created at the end device when the user logs in to the system. The profile is retained at the end device even when the user logs out and based on the profile management configurations.

> **Note:**
>
> With the Desktop Lock installed, and `LiveInDesktopDisconnectOnLock` set to **False** in the registry path `HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\Dazzle` Or `HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Citrix\Dazzle`, the active session gets disconnected when the end-point wakes up from hibernation or standby mode.

Install Citrix Workspace app Desktop Lock

This procedure installs Citrix Workspace app for Windows so that virtual desktops appear using Citrix Workspace app Desktop Lock. For deployments that use smart cards, see Smart card.

1. Log on using a local administrator account.
2. At a command prompt, run the following command:

   For example:

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

   The command is available in the Citrix Workspace app and **Plug-ins** > **Windows** > **Citrix Workspace app** folder on the installation media. For command details, see the Citrix Workspace app install documentation at Install.
3. In the same folder on the installation media, double-click `CitrixWorkspaceDesktopLock.msi`. The Desktop Lock wizard appears. Follow the prompts.
4. When the installation completes, restart the user device. If you have permission to access a desktop and you log on as a domain user, the device appears using Citrix Workspace app Desktop Lock.

You can allow administration of the user device after installation, the account used to install `CitrixWorkspaceDesktopLock.msi` is excluded from the replacement shell. If that account is later deleted, you can't log on and administer the device.

To run a **silent install** of Citrix Workspace Desktop Lock, use the following command line:

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

Configure Citrix Workspace app Desktop Lock

When you've logged in as a non-administrator, Desktop Lock automatically launches an assigned desktop session.

Using Active Directory policies prevent users from hibernating virtual desktops.

Use the same administrator account to configure Citrix Workspace app Desktop Lock as you did to install it.

- Check if the receiver.admx (or receiver.adml) and receiver_usb.admx (.adml) files are loaded into Group Policy (where the policies appear in Computer Configuration or **User Configura-**

tion > **Administrative Templates** > **Classic Administrative Templates (ADMX)** > **Citrix Components**). The .admx files are in %Program Files%\Citrix\ICA Client\Configuration\.

- USB preferences - When a user plugs in a USB device, that device is automatically remoted to the virtual desktop and no user interaction is required. The virtual desktop controls the USB device and displaying it in the user interface.
  - Enable the USB policy rule.
  - In **Citrix Workspace app** > **Remoting client devices** > **Generic USB Remoting**, enable and configure the Existing USB Devices and New USB Devices policies.
- Drive mapping - In **Citrix Workspace app** > **Remoting client devices**, enable, and configure the Client drive mapping policy.
- Microphone - In **Citrix Workspace app** > **Remoting client devices**, enable, and configure the Client microphone policy.

Configure smart cards for use with Windows Desktop Lock

1. Configure StoreFront.
   a) Configure the XML Service to use DNS Address Resolution for Kerberos support.
   b) Configure StoreFront sites for HTTPS access, create a server certificate signed by your domain certificate authority, and add HTTPS binding to the default website.
   c) Make sure that pass-through authentication with the smart card is enabled (enabled by default).
   d) Enable Kerberos.
   e) Enable Kerberos and pass-through authentication with smart card.
   f) Enable Anonymous access on the IIS Default website and use Integrated Windows Authentication.
   g) Ensure that the IIS Default website doesn't require SSL and ignores client certificates.
2. Use the Group Policy Management Console to configure Local Computer Policies on the user device.
   a) Import the Receiver.admx template from %Program Files%\Citrix\ICA Client\Configuration\.
   b) Expand **Administrative Templates** > **Classic Administrative Templates (ADMX)** > **Citrix Components** > **Citrix Workspace** > **User authentication**.
   c) Enable Smart card authentication.
   d) Enable Local user name and password.
3. Configure the user device before installing Citrix Workspace app Desktop Lock.
   a) Add the URL for the Delivery Controller to the Windows Internet Explorer Trusted Sites list.
   b) Add the URL for the first Delivery Group to the Internet Explorer Trusted Sites list. Add the URL in the form desktop://delivery-group-name.

c) Enable Internet Explorer to use automatic logon for Trusted Sites.

When Citrix Workspace app Desktop Lock is installed on the user device, it enforces a consistent smart card removal policy. For example, if the Windows smart card removal policy is set to Force logoff for the desktop, the user must log off from the user device, regardless of the Windows smart card removal policy set on it. Desktop Lock ensures that the user device isn't left in an inconsistent state. This applies only to user devices with the Citrix Workspace app Desktop Lock.

Remove Desktop Lock

Be sure to remove both of the components listed as follows:

1. Log on with the same local administrator account that was used to install and configure Citrix Workspace app Desktop Lock.
2. From the Windows feature for removing or changing programs:
    - Remove Citrix Workspace app Desktop Lock.
    - Remove Citrix Workspace app for Windows.

Passing Windows shortcut keys to the remote session

Most windows shortcut keys are passed to the remote session. This section highlights some of the common ones.

Windows

- Win+D - Minimize all windows on the desktop.
- Alt+Tab - Change active window.
- Ctrl+Alt+Delete - via Ctrl+F1 and the Desktop Viewer toolbar.
- Alt+Shift+Tab
- Windows+Tab
- Windows+Shift+Tab
- Windows+All Character keys

Windows 8

- Win+C - Open charms.
- Win+Q - Search charm.
- Win+H - Share charm.
- Win+K - Devices charm.

- Win+I - Settings charm.
- Win+Q - Search apps.
- Win+W - Search settings.
- Win+F - Search files.

Windows 8 apps

- Win+Z - Get to app options.
- Win+. - Snap app to the left.
- Win+Shift+. - Snap app to the right.
- Ctrl+Tab - Cycle through app history.
- Alt+F4 - Close an app.

Desktop

- Win+D - Open desktop.
- Win+, - Peek at desktop.
- Win+B - Back to desktop.

Other

- Win+U - Open Ease of Access Center.
- Ctrl+Esc - Start screen.
- Win+Enter - Open Windows Narrator.
- Win+X - Open the system utility settings menu.
- Win+PrintScrn - Take a screenshot and save to pictures.
- Win+Tab - Open switch list.
- Win+T - Preview open windows in taskbar.

Software Development Kit (SDK) and API

October 7, 2023

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

October 7, 2023

> **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\Inst
On a 64-bit machine	[HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\Citrix\A

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

On a 32-bit machine	[HKEY_CURRENT_USER\SOFTWARE\Citrix\AuthManager\Insta
On a 64-bit machine	[HKEY_CURRENT_USER\SOFTWARE\WOW6432Node\Citrix\Au

Requirements

- 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
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>
```

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 0
x2000 –E <https://my.firstexamplestore.net/Citrix/Store/discovery>
```

Command example on Citrix Gateway:

```
.\storebrowse.exe –U { Username } –P { Password } –D { Domain } –M 0
x2000 –E <https://my.secondexample.net>
```

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
```

The name that is in bold in the previous output is used as an input parameter to the launch option.

Command example on StoreFront:

```
.\storebrowse.exe -U { Username } –P { Password } –D { Domain } –L
“{ Resource_Name } <https://my.firstexamplestore.net/Citrix/Store/
discovery>
```

Command example on Citrix Gateway:

```
<.\storebrowse.exe –U { Username } –P { Password } –D { Domain } –L {
Resource_Name } https://my.secondexamplestore.com>
```


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 store0-5
    c3ec017 -CitrixID store0-5c3ec017@@a9a8e3ac-099d-4577-b84e-
    e33d0695df39.Notepad -ica "https://cwawiniwstest.cloudburrito.com/
    Citrix/Store/resources/v2/
    YTlhOGUzYWMtMDk5ZC00NTc3LWI4NGUtZTMzZDA2OTVkZjM5Lk5vdGVwYWQ-/launch/
    ica" -cmdline

<!--NeedCopy-->
```

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.

Storebrowse for Workspace

November 28, 2023

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/YTlhOGUzYWMtMDk5ZC00NTc3LWI4NGUtZTMzZDA2OTVkZjM5Lk5
-/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

December 26, 2023

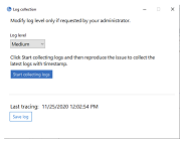
Log collection

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.

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.

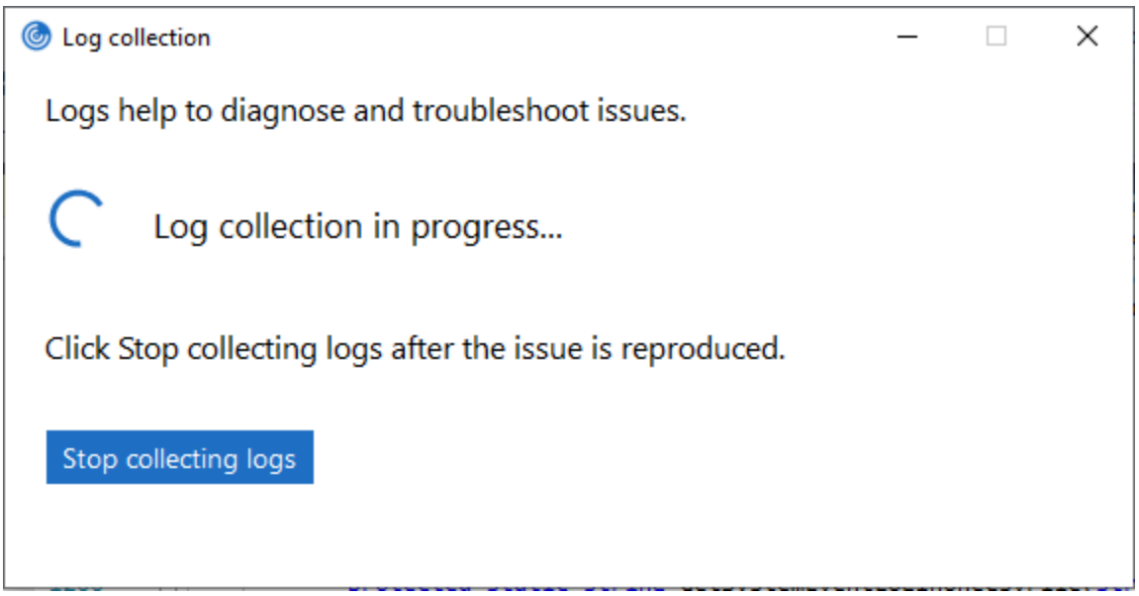


3. Select one of the following log levels:

    - 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

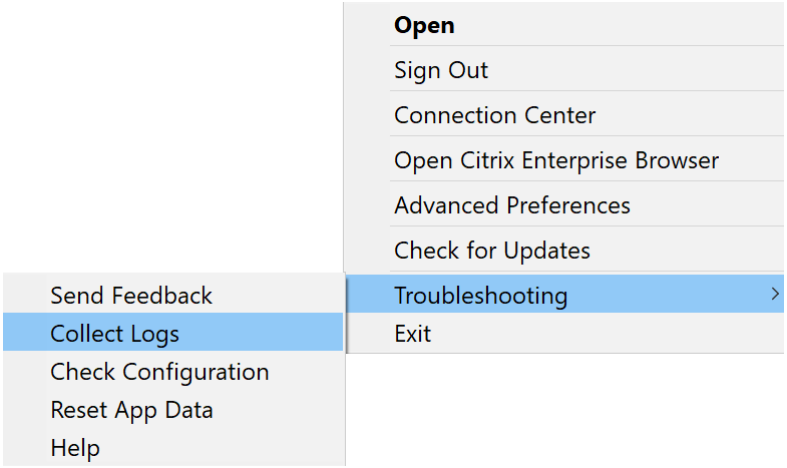
- HDX
- Receiver shell, Auth Manager, and Self-Service plug-in
- Install logs
- Always-On logs

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

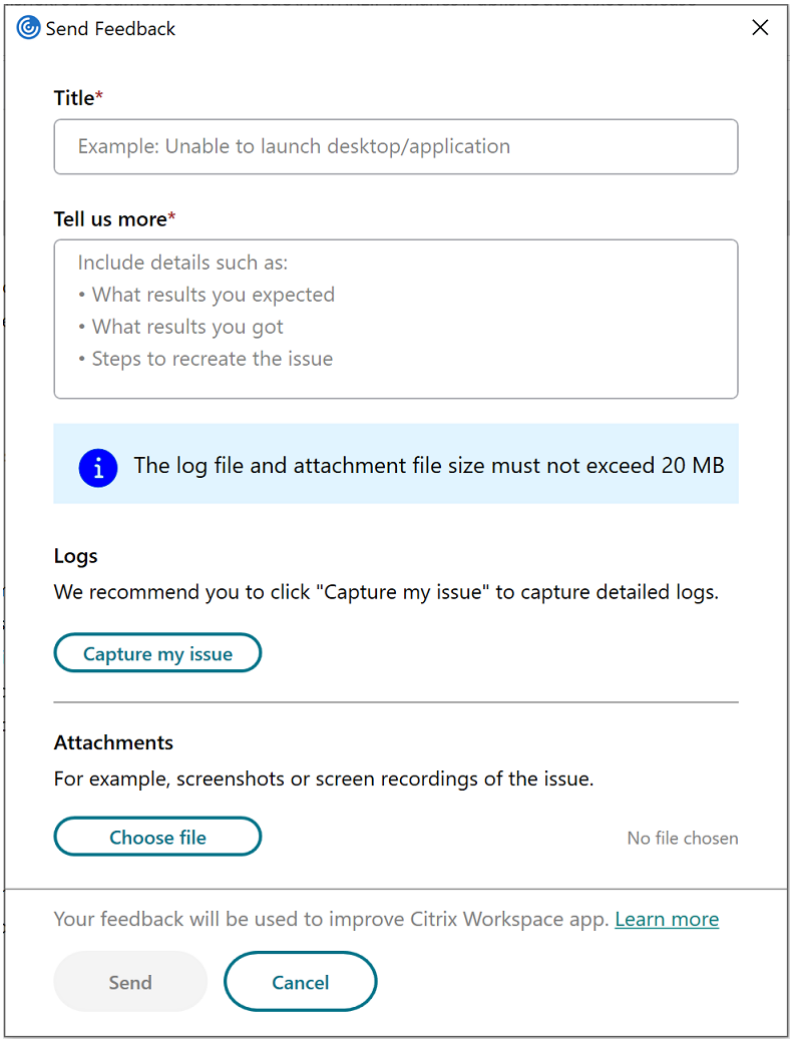


Send feedback on Citrix Workspace app

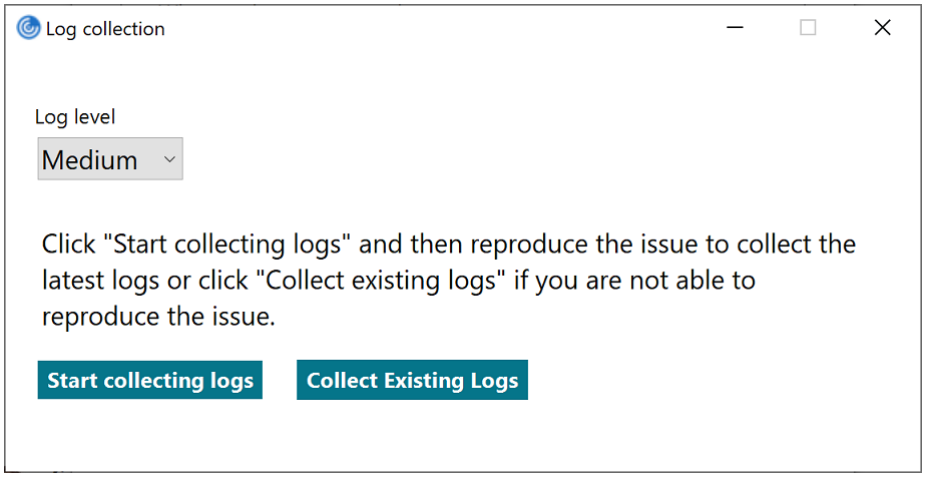
The **Send feedback** option allows you to inform Citrix about any issues that you might run into while using Citrix Workspace app. You can also send suggestions to help us improve your Citrix Workspace app experience.

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.

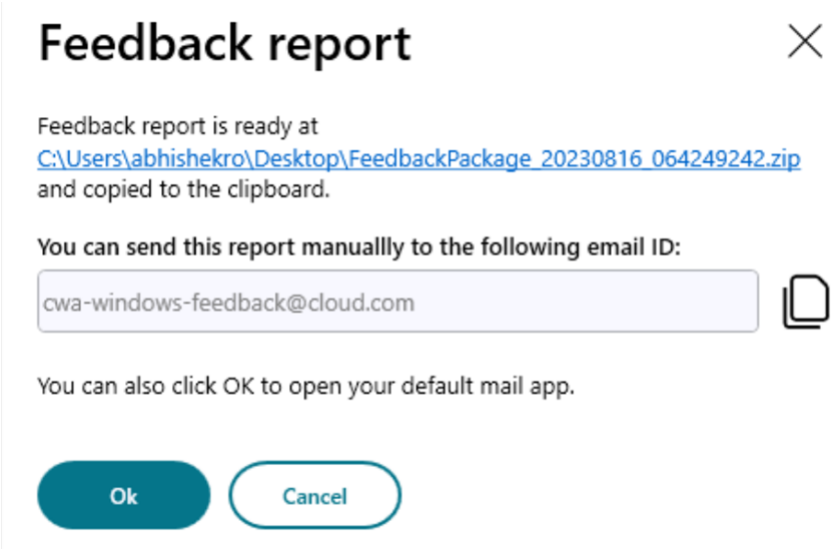
b) Click **Stop collecting logs** after the issue is reproduced.

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.

Deprecation

February 7, 2024

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
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.

Item	Deprecation announced in	Removed in	Alternative
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 Workspace 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 with Citrix Workspace app	2112.1	2205	Citrix Casting can be installed on-demand 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	

Item	Deprecation announced in	Removed in	Alternative
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** Windows 7 is supported in Version 2002.
`/rcu` installer switch	1909		Use `/forceinstall` switch instead of `/rcu`.