Client app management

Contents

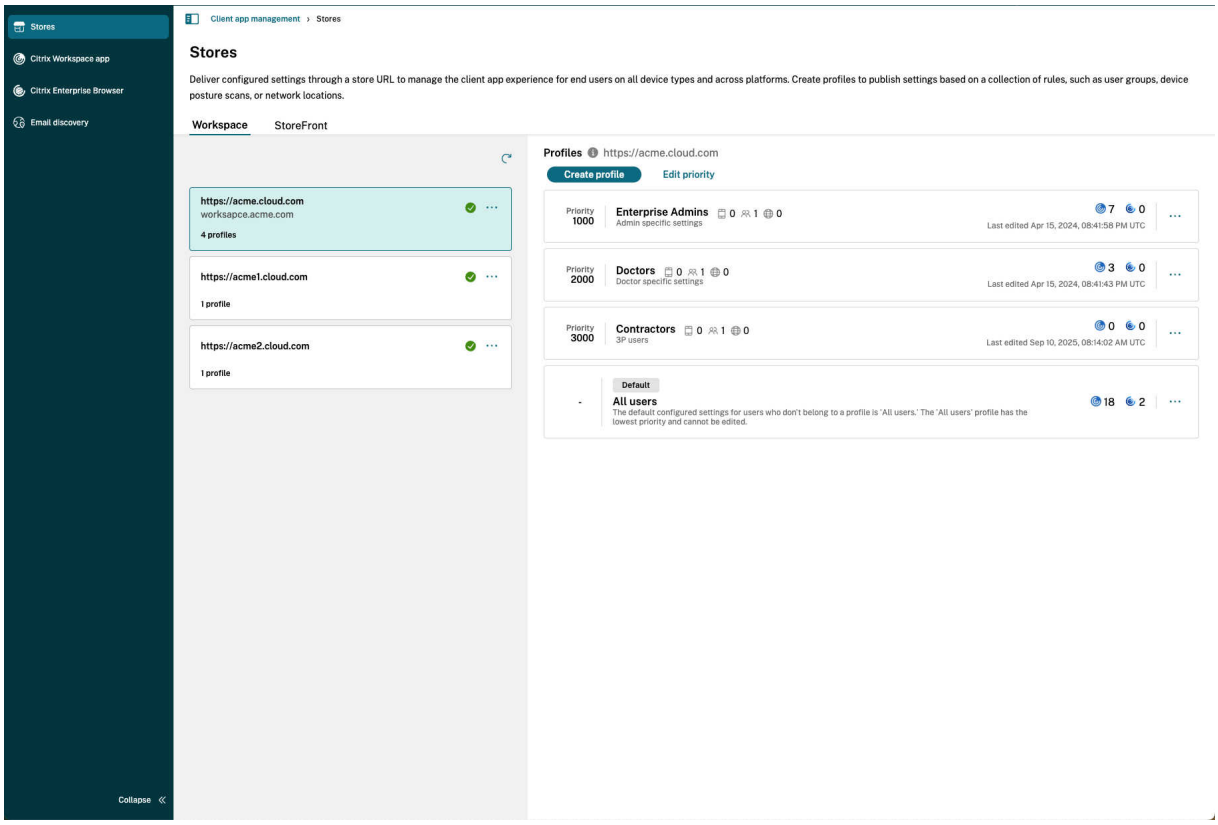
Client app management

October 16, 2025

Client app management (previously known as the Global App Configuration Service), is a cloud service designed to provide a single, centralized place for administrators to manage the settings of various Citrix client applications.

This service allows administrators to define and distribute configurations for a specific Store URL. It's designed to be highly flexible and work across various environments:

- **Deployment Types**
  - Cloud (Citrix Workspace)
  - On-premises (Citrix StoreFront)
- **Device Types**
  - Managed
  - Unmanaged (Bring Your Own Device)
- **Operating Systems**
  - Windows, Mac, HTML5, ChromeOS, Android, iOS, and Linux.



Supported Client Applications

You can manage settings for the following Citrix applications:

- Citrix Workspace app
- Citrix Enterprise Browser

Key benefits of Client app management

Client app management offers a robust set of features to streamline administration.

Centralized Configuration

- **Manage Multiple URLs**: Onboard and manage multiple StoreFront, gateway, or workspace URLs from a single cloud tenant.
- **Granular Control**: For each URL, you can manage specific settings for the Citrix Workspace app, and Citrix Enterprise Browser.
- **Configuration profiles**: Create specific configuration profiles for each URL. These profiles allow you to apply different settings based on contextual policies, such as:
  - User groups
  - Device Posture service rules
  - Network Location service rules

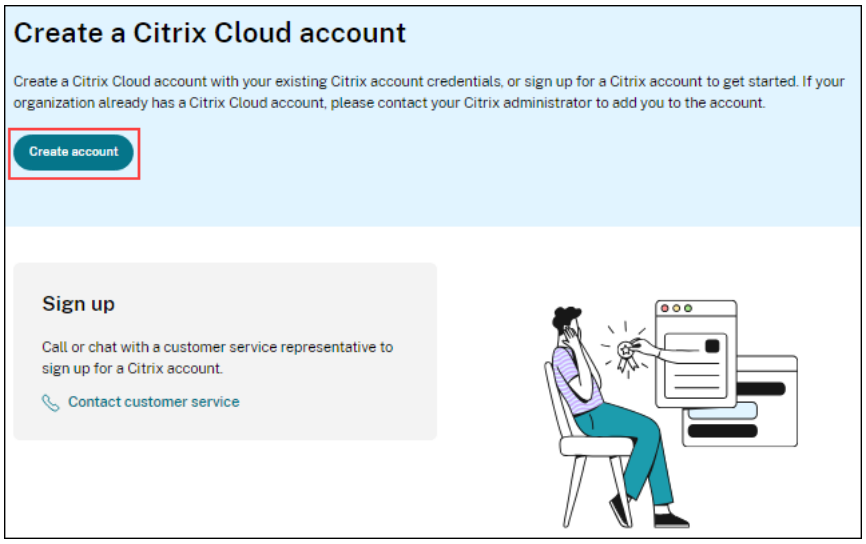
Simplified Rollouts and Management

- **Test and Production Channels**: Easily switch between a test channel and a production channel for each store URL, allowing you to validate changes before a full rollout.
- **Detailed Settings View**: Access a detailed view for each setting that includes descriptions, supported client versions, dependencies on other settings, and default behaviors.
- **Smart Categorization**: Settings are highlighted as "recommended," "new," or "legacy" to guide administrators.
- **Powerful Search and Filtering**: Quickly find specific settings or profiles by filtering based on:
  - Platform (for example, Windows, Mac, and so on)
  - Category of settings
  - Description of a setting

Onboard to Client app management

September 30, 2025

To get started with Client app management, verify that you have access to a Citrix Cloud account. If not, you can create an account from https://onboarding.cloud.com/. For more information, refer to Sign up for Citrix Cloud.



> **Important:**
>
> The following addresses must be contactable from the client for the functioning of email-based discovery and Client app management:
>
> - https://discovery.cem.cloud.us
> - https://gacs-discovery.cloud.com
> - https://gacs-config.cloud.com

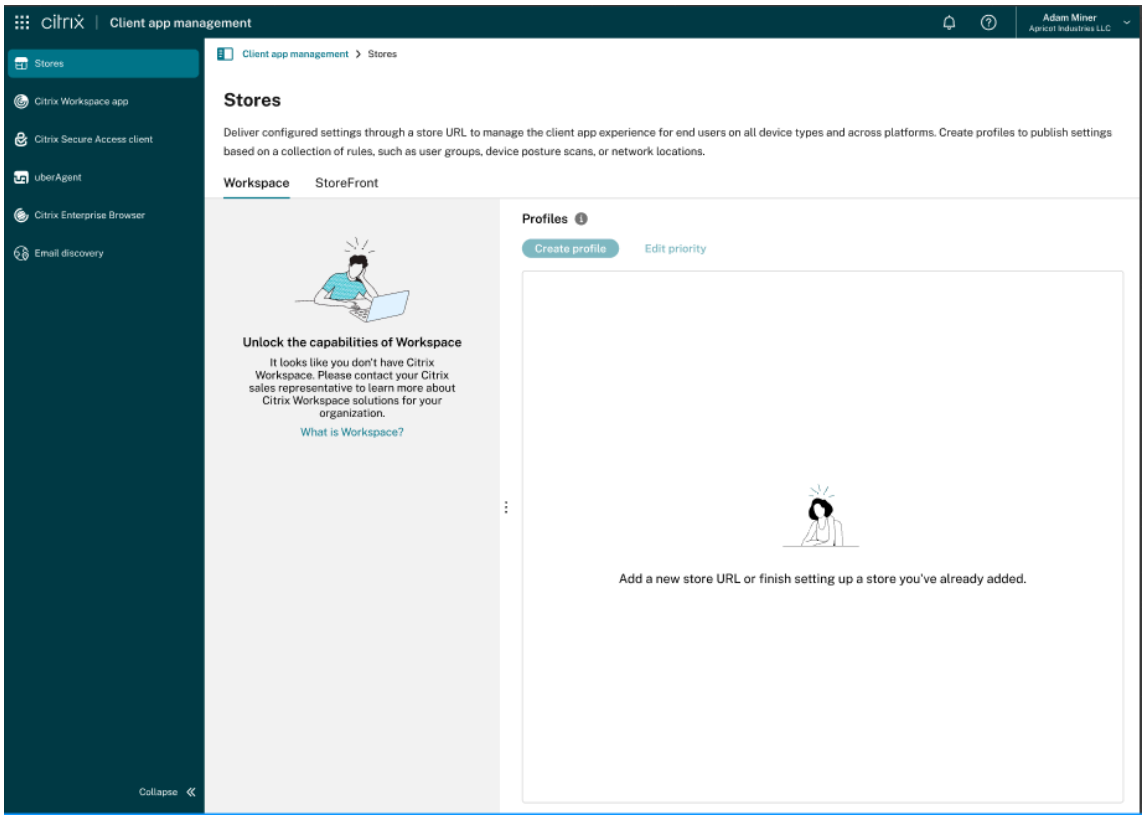
Workspace

September 30, 2025

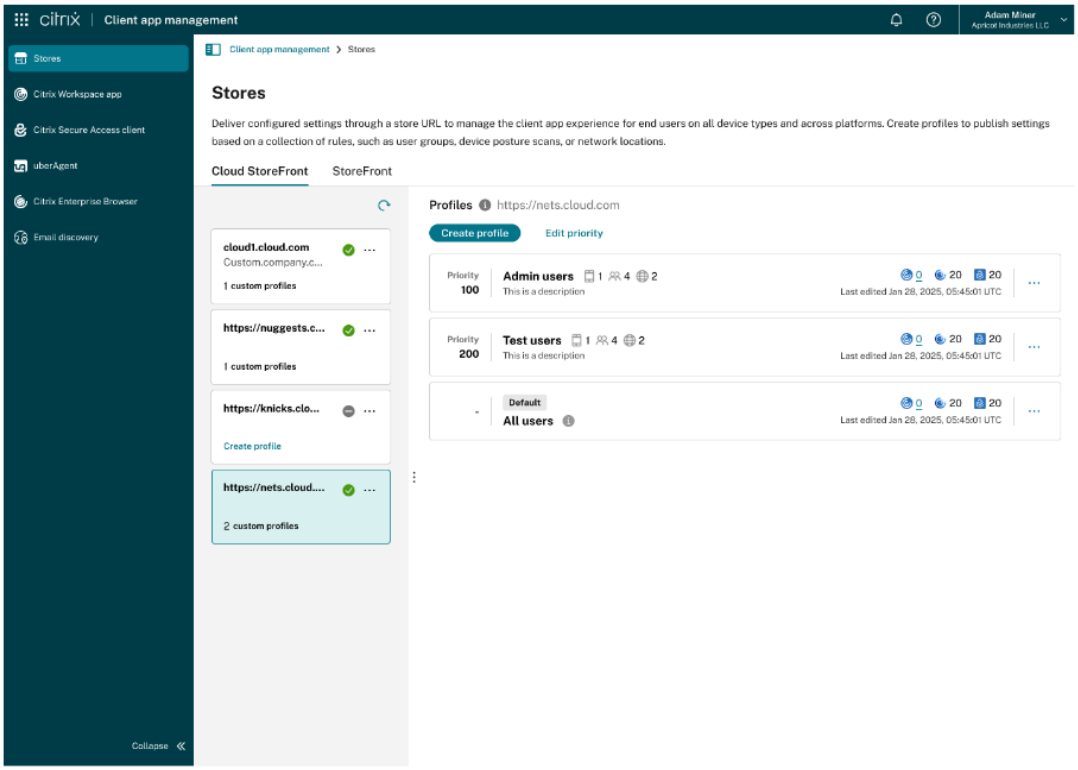
You can sign in to your Citrix Cloud account and access **Client app management** from the main menu. Before proceeding, verify if you have the following permissions:

- **Workspace subscription:** The Workspace subscription is required to create a Workspace URL. If you don't have a subscription, you can't add and configure cloud stores.

- **Workspace URL:** If you have a Workspace subscription but haven't added your URL yet, you must set up the store to get started.



- If you have a Workspace URL already configured, you see the list of cloud store URLs. This means that you are good to get started with the configuration.



Configure settings for custom domains

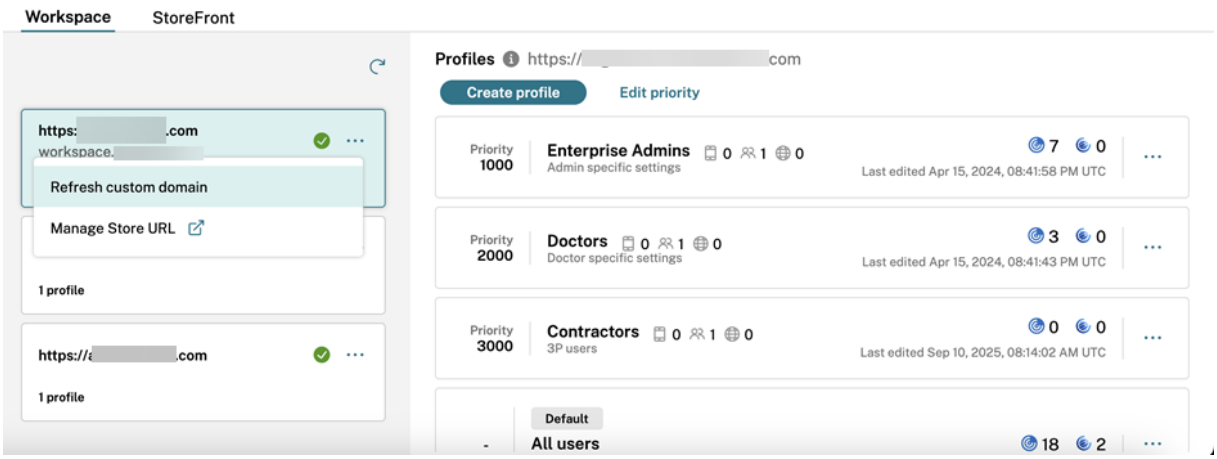
You can apply the Client app management settings to *custom domain URLs* in addition to *cloud.com* domain URLs. After you enable this mapping in the UI, any user accessing the store through a custom domain receives settings configured for the corresponding *cloud.com* based store.

For more information about custom domains, see Configure a custom domain.

Workflow to enable settings for custom domain

To enable Client app management settings for custom domains, perform the following:

1. Navigate to **Client app management** > **Stores** > **Workspace**.
2. Locate the three dots next to each Workspace URL.
3. Click **Refresh custom domain**, if a custom domain is configured for the Workspace URL.



The system fetches and populates the mapping between your *custom domain* and the *cloud.com* URL in the column.

Points to remember For settings to take effect on custom domains:

1. Settings might take up to 24 hours to apply for already logged-in users on the Citrix Workspace™ app.
2. Wait for 30 minutes after mapping the *custom domain* to the *cloud.com* URL in Client app management.

Compatibility The following Citrix Workspace app versions support this feature:

Windows: Version 2503.10 or later

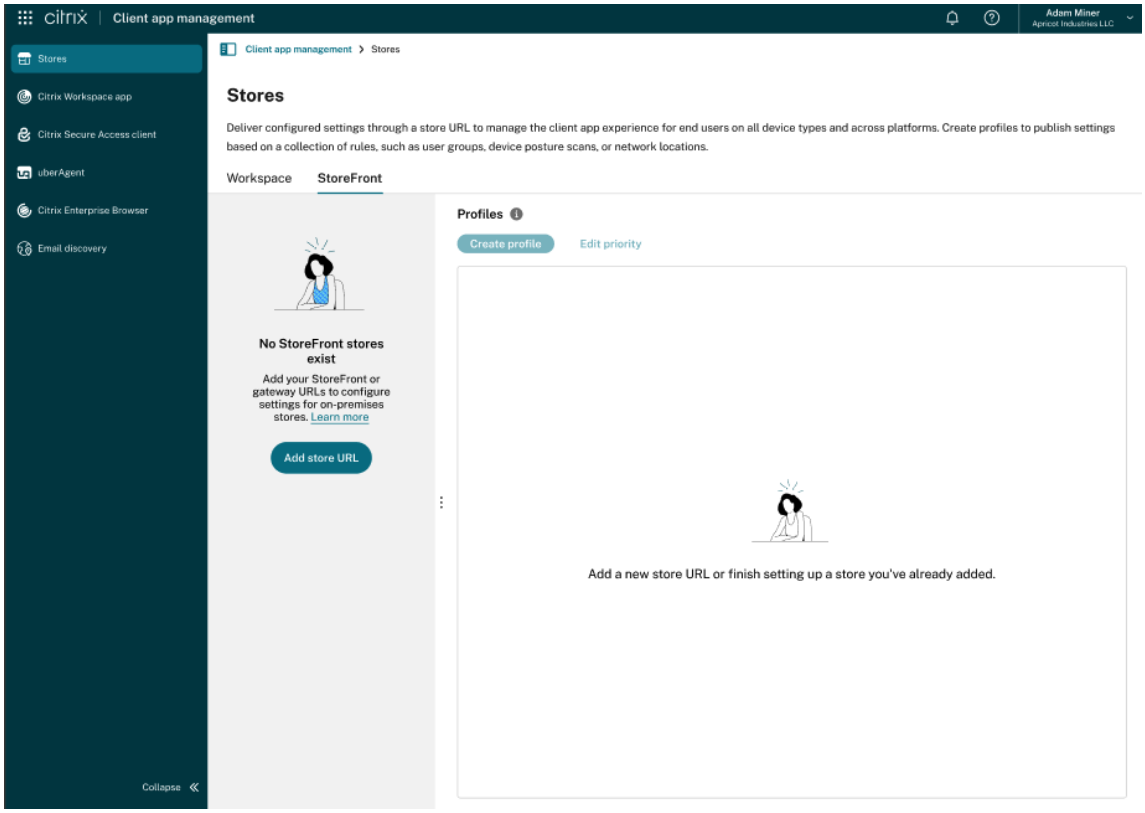
Mac: Version 2503 or later

StoreFront

October 16, 2025

You need to verify the ownership of your Store URL to get started with Client app management.

1. Navigate to **Client app management** > **Stores** > **StoreFront**.
2. If you don't have any StoreFront URL claimed, you are presented with the following screen:



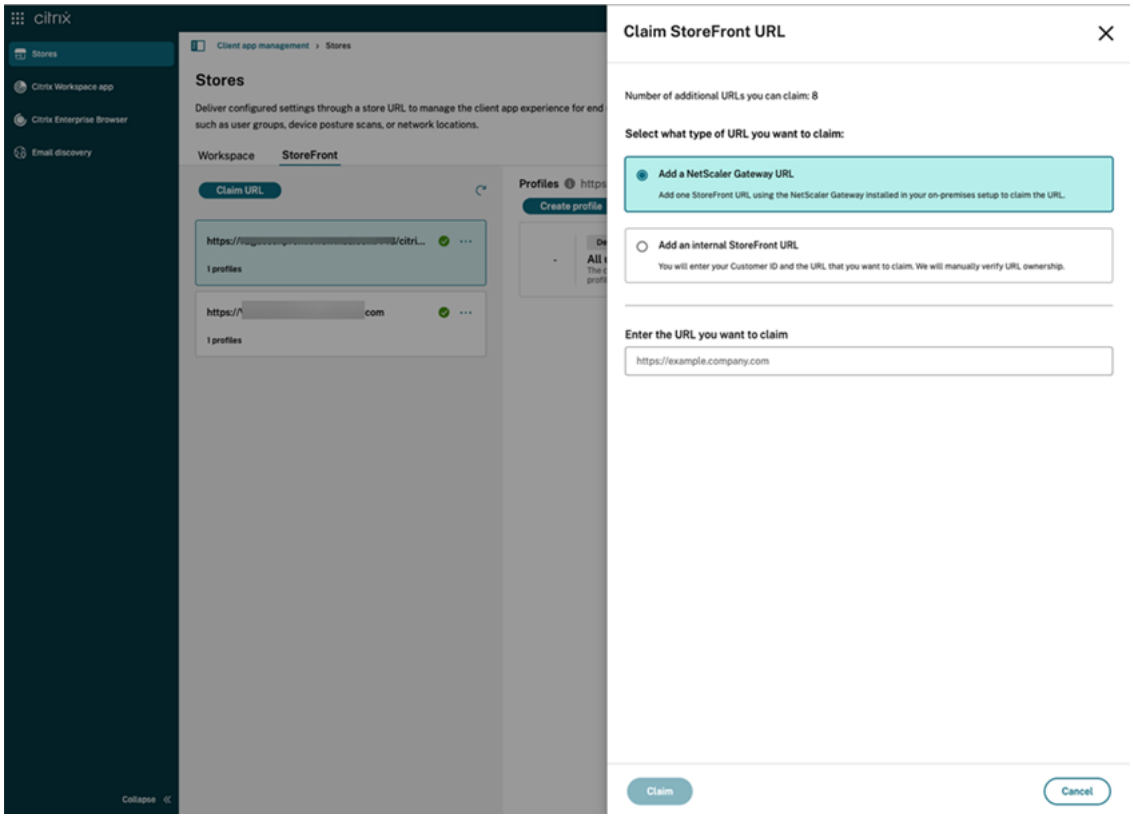
You can claim the URLs for the following store access mechanism:

- **Gateway URL (Recommended)** - Using Gateway URL is the preferred method for claiming a store's URL. It acts as a single point of entry, simplifying access for users and providing a consistent experience.
- **Internal StoreFront URL** - Used for internal access, this URL is typically for employees or administrators within a private network.
- **Custom Web store** - Custom Web store URL must be claimed if a customer has a highly customized StoreFront store.

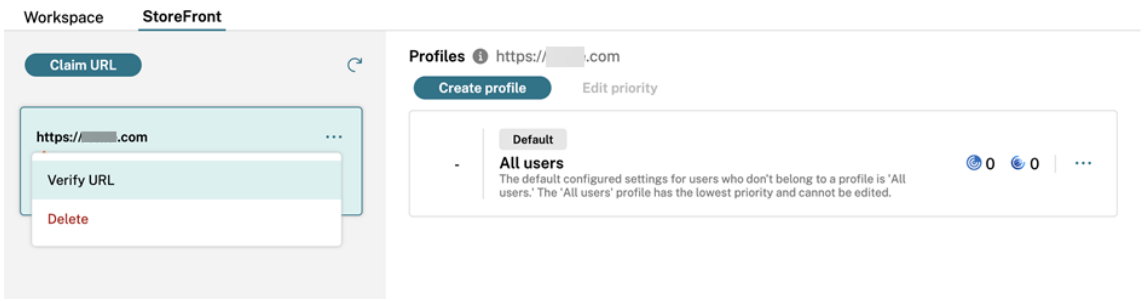
Claim a Gateway URL for StoreFront stores

To claim a Gateway URL:

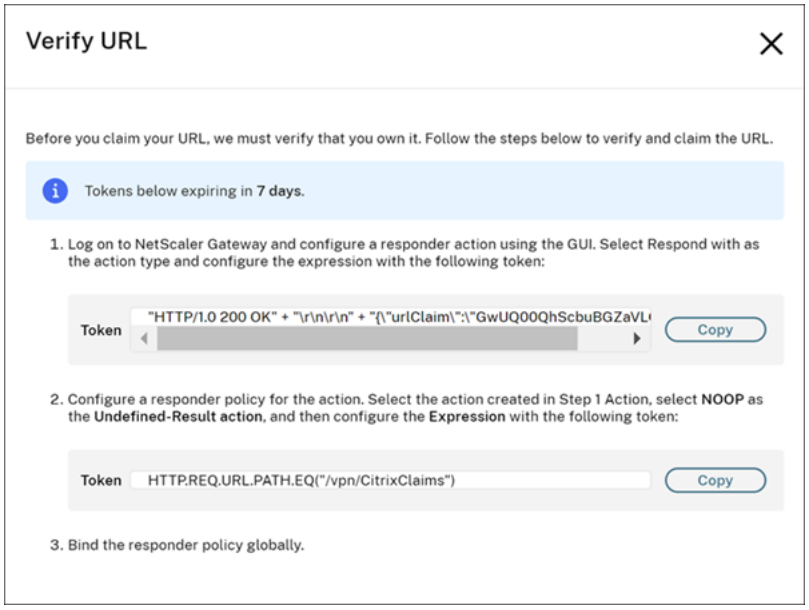
1. Sign in to **Citrix Cloud**.
2. From the main menu, navigate to **Client app management** > **Stores**.
3. Click **StoreFront** > **Claim URL**.
4. Select **Add a NetScaler Gateway URL**.



5. Enter the URL in the given text field and click **Claim**. The URL is added, and it is in the **'Verification not started'** state.
6. To verify the URL, select the URL and click **Verify URL**.



7. The **Verify URL** screen contains the steps that guide you to create and configure a responder action and responder policy within your NetScaler.



a) Bind your responder policy globally.

b) Go to `https://<customergatewayurl>/vpn/CitrixClaims` to verify if your responder policy is configured correctly.

c) Navigate back to **Workspace configuration** > **App configuration**, and locate the URL that you added.

d) Select the URL and click **Verify URL**.

e) Click **Verify URL** to start the verification process.

> **Note:**
>
> The URL verification process is initiated once you click **Verify URL** and takes approximately 15 minutes to complete.

To claim an internal StoreFront URL

If your store cannot be accessed over the internet or through a public gateway URL, you might request for an exception with your store details. You can raise a support ticket with Citrix if necessary.

To claim a custom webstore URL

Citrix Workspace app supports custom web stores that allow end user to connect to stores that are customized based on their company themes.

If you want to configure settings against a custom web store URL, you can claim the URL via a direct request using the Client app management API endpoints. Learn more here.

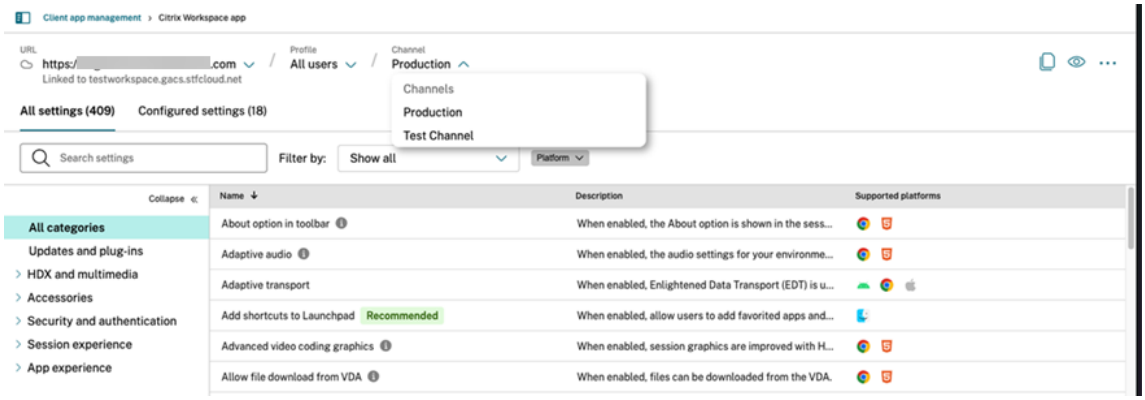
Test channel configuration

September 30, 2025

You can test your configuration before enabling it for the end users. It helps you detect and resolve any issues that might arise post deployment. The testing capability significantly reduces the likelihood of disruptions or errors during the deployment process and increases overall user satisfaction.

To test your configuration:

1. Go to the cloud portal and sign in with your Citrix Cloud credentials.
2. Navigate to **Client app management** > **Stores**.
3. From the list of configured store URLs, select the store for which you want to map settings and then click **Configure**.
4. Click the drop-down list option and select **Test Channel**. It is set to **Production** by default.



5. Modify the settings for your preferred platforms as per your requirement.
6. You can then click **Publish Drafts** to publish your settings in the test channel.

> **Note:**
>
> Client app management supports only two channels per store, one production (default) and one test channel.

Configure channel support on end-user devices

Windows

To test the configuration defined by admins on a Windows device, users need to create the following registry:


```
Path - HKEY_CURRENT_USER\SOFTWARE\Citrix\Receiver
Name - AppConfigChannelName
Type - REG_SZ
Value - testrolloutchannel1
```

Mac

To test the configuration defined by the admin on a Mac device, users need to perform the following steps:

1. Set the name of the Client app management test channel using the following command:

   ```
   defaults write com.citrix.receiver.nomas GACSChannelName
       testrolloutchannel1
   ```

2. Restart the **Citrix Workspace™ Helper**, using the following commands:

   ```
   launchctl unload /Library/LaunchAgents/com.citrix.ReceiverHelper.
       plist
   launchctl load /Library/LaunchAgents/com.citrix.ReceiverHelper.
       plist
   ```

After the device restarts, the configuration for the test channel is fetched automatically.

iOS

To test the configuration defined by the admin on an iOS device, proceed as follows:

1. Sign in to the **Citrix Workspace App**.
2. Go to **Settings** > **Advanced** > **App configuration**.
3. Select the test channel.

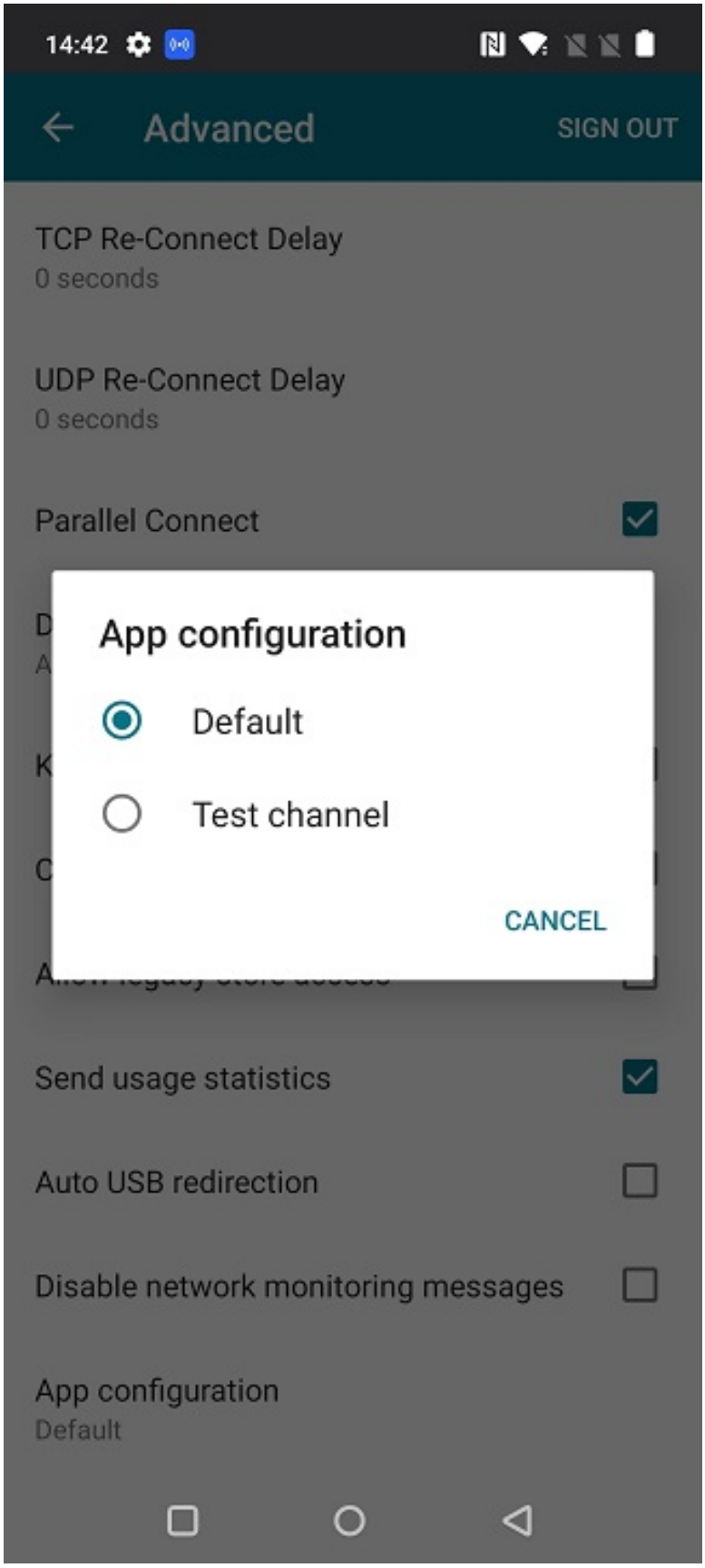
   You can now test the configuration defined by the admin.

Android

To test the configuration defined by the admin on an Android device, proceed as follows:

1. Sign in to **Citrix Workspace app**.
2. Go to **Settings** > **Advanced** > **App Configuration**.
3. Select the test channel.

   You can now test the configuration defined by the admin.



Manage settings for a store URL

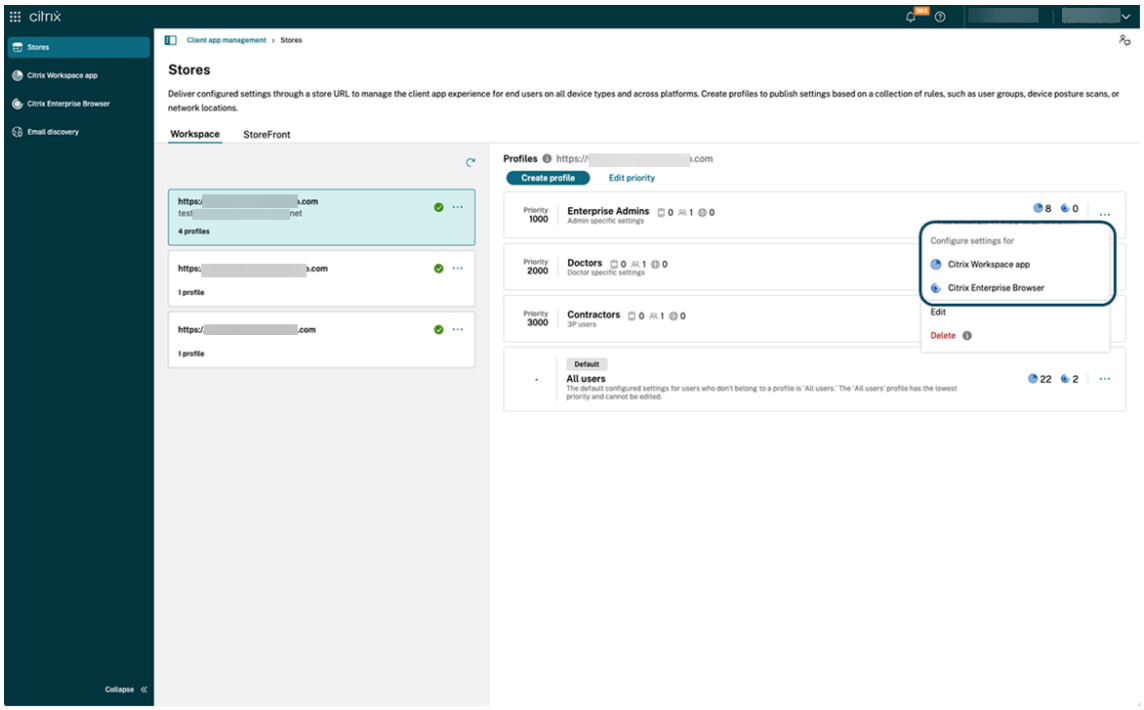
October 17, 2025

The following section explains how to configure settings for a store URL across Citrix client applications.

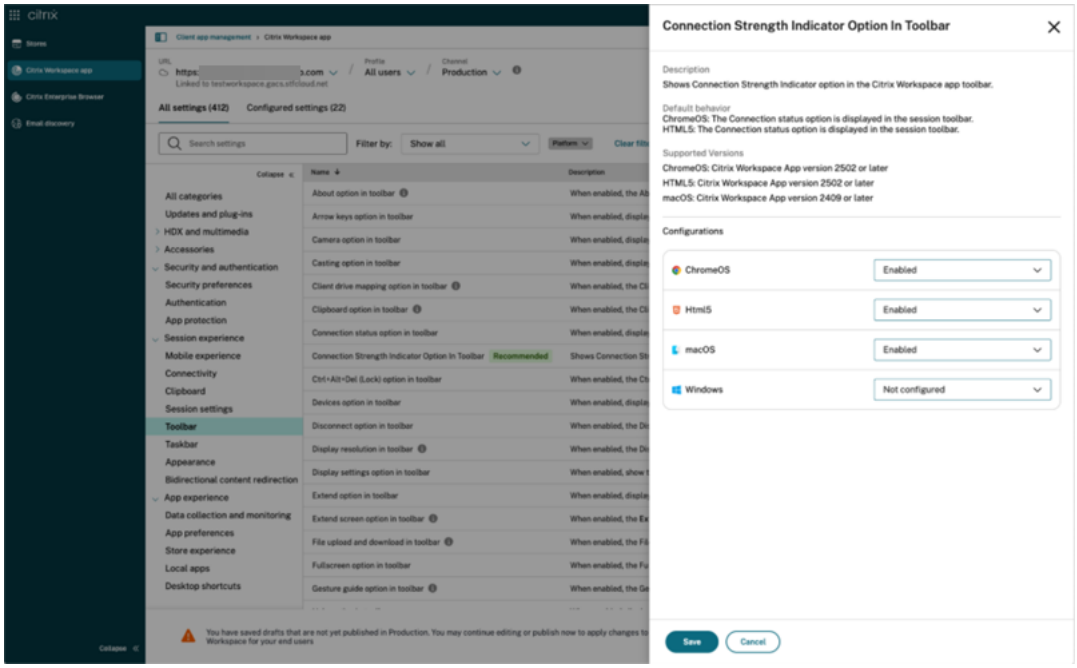
How to configure settings

To configure settings:

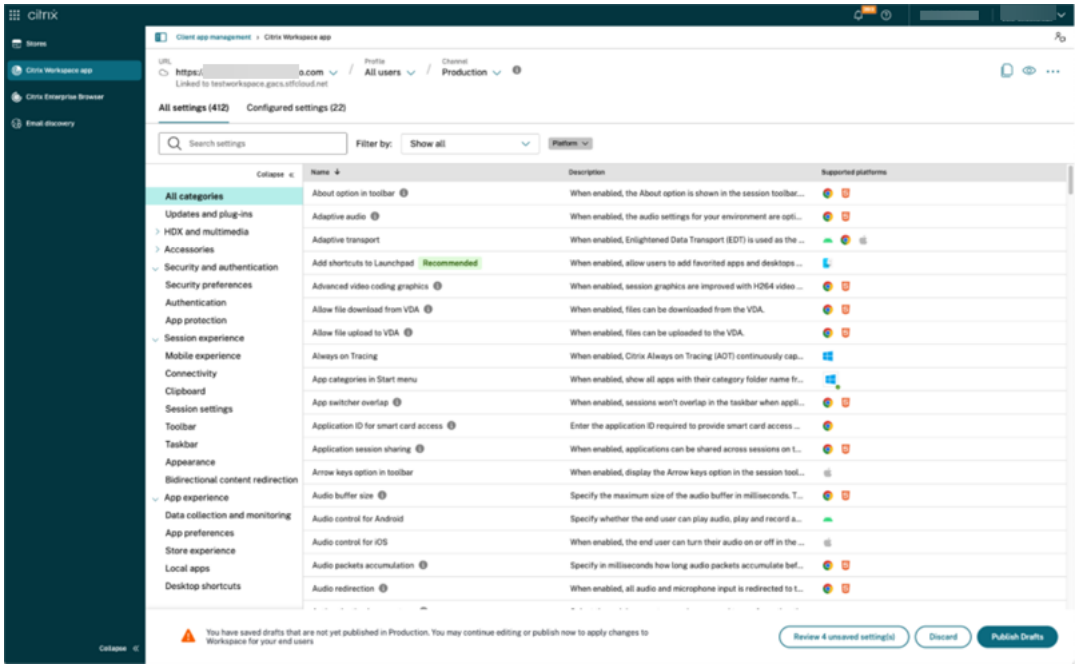
1. Sign in the **Citrix Cloud** portal and navigate to **Client app management**.
2. From the list of configured store URLs, select the store for which you want to map settings.
3. Click three dots next to the store URL and choose the client app for which you want to configure the settings.



4. Modify the app settings as per your organization's policies and click **Save**.



5. Click **Publish Drafts** to save and publish your settings.

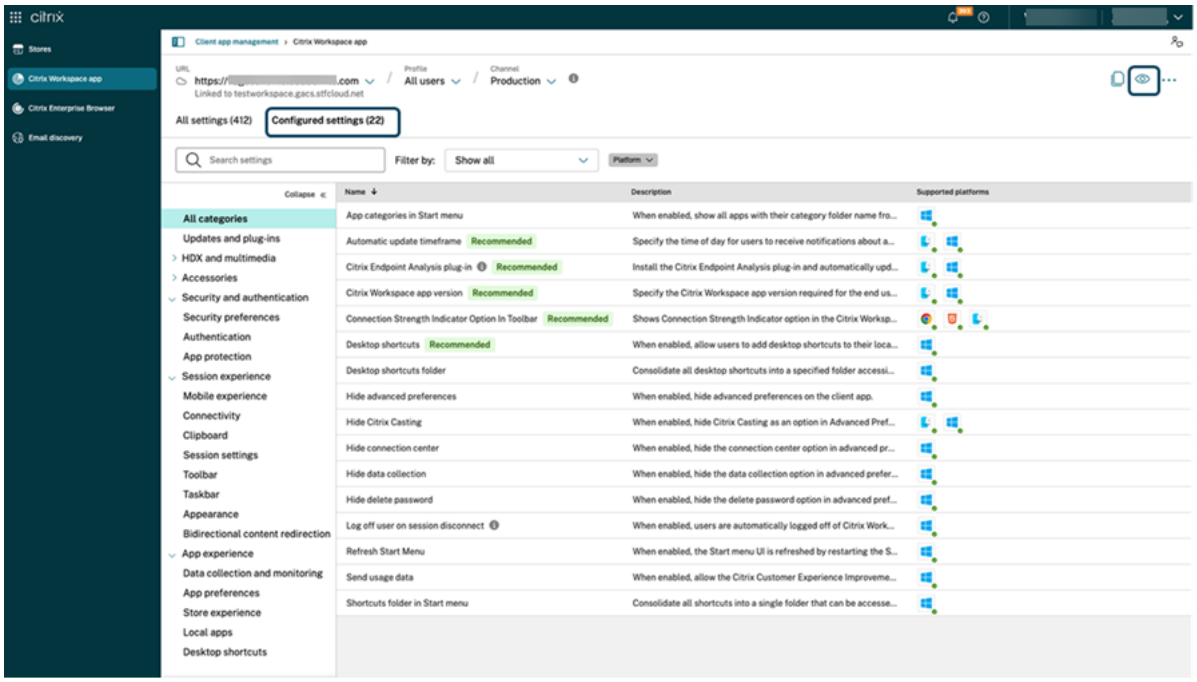


The user interface also provides the following options for a simplified user experience.

View a summary of configured settings

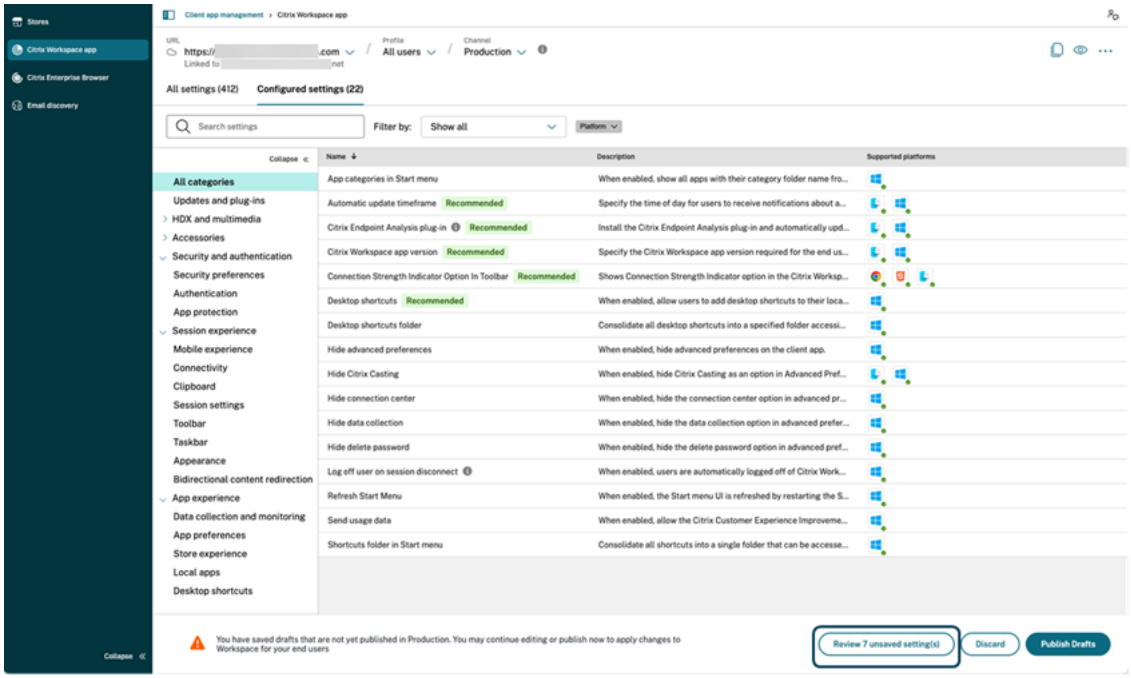
You can view a summary of the current configuration by clicking **Configured settings** tab. It eliminates the need to expand and review each setting separately. A consolidated list of all the configured

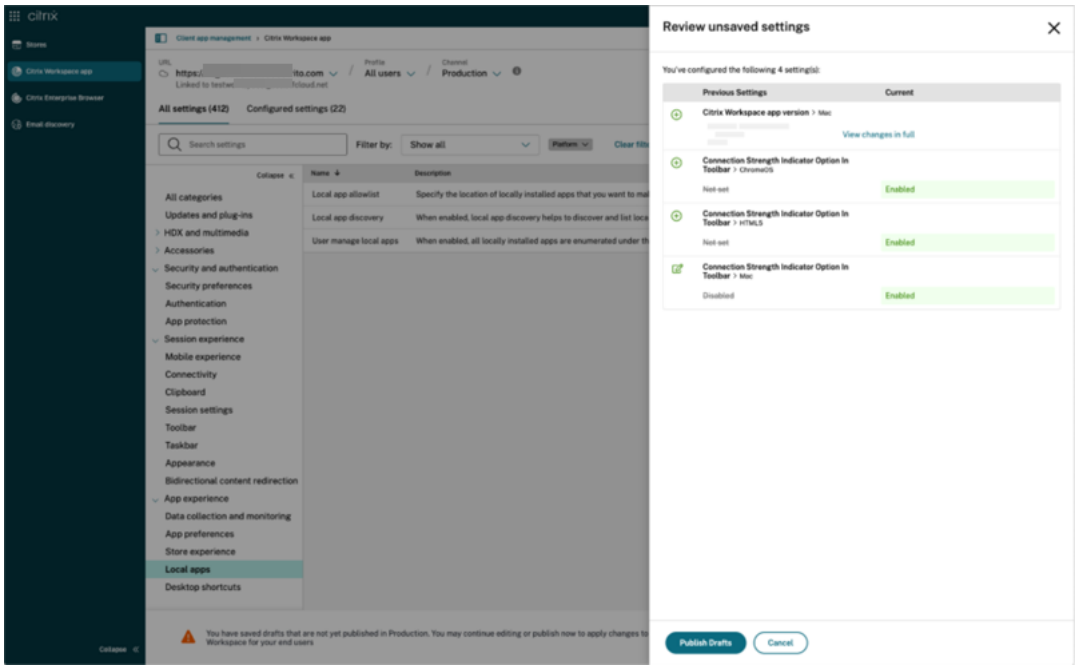
settings allows you to perform a comprehensive review of the current configuration and gauge the user impact. As an alternative, you can also click the **View configured settings** icon as shown in the following screenshot.



Review unsaved changes

Perform a final review of your unsaved changes before publishing the configuration. The number of unsaved settings is displayed on the UI and you can access this list by clicking the **Review unsaved setting(s)** option. It enables you to make informed changes and maintain data accuracy.





Enhanced search option

The search experience has been enhanced to provide a robust and seamless experience. Admins can now sign in to the cloud portal and locate the required settings on the Client app management page with ease. They can use the following search methods.

Search using setting description

You can locate settings by entering keywords found within the setting's description. It allows for a more flexible search approach, using relevant terms associated with the desired setting.

Search using API setting name

You can search for settings by entering the corresponding API setting name. This method allows for a more precise and targeted search, enabling users to quickly find the specific setting they require.

View applicable platforms for each setting

Each setting now dynamically displays only those platforms to which it's relevant and applicable. This approach ensures that users are presented with a concise and tailored list of options.

Introduction to profiles

October 17, 2025

A profile allows administrators to deliver settings based on a collection of rules, based on user groups, device posture scans, or network locations.

- User groups based on Identity Providers (IdP)

  A *user group* is a collection of users managed by administrators, often defined in your organization's identity provider (such as Active Directory). Grouping users allows you to apply settings and policies to multiple users at once. For more information, see the section Configure Authentication.

- Device posture service (DPS) policies

  Device posture refers to the security and health status of a device. You need to configure device posture rules and use the policy name as a tag in the config. This policy name is set in the **create device policy** section. Both the compliance result and the device name can be used as criteria. For more details, see the section Configure Device Posture.

- Network Location service (NLS) policies

  A *network location* is a policy that determines user access based on their network connection, such as being on an internal or public network. Network location tags are available in the dropdown list when configuring a profile. If you haven't configured network locations yet, set them up as described in Configure Network Location.

Profile Types

Admin-enforced rules determine which profile type applies to users. User profiles fall into one of the following categories:

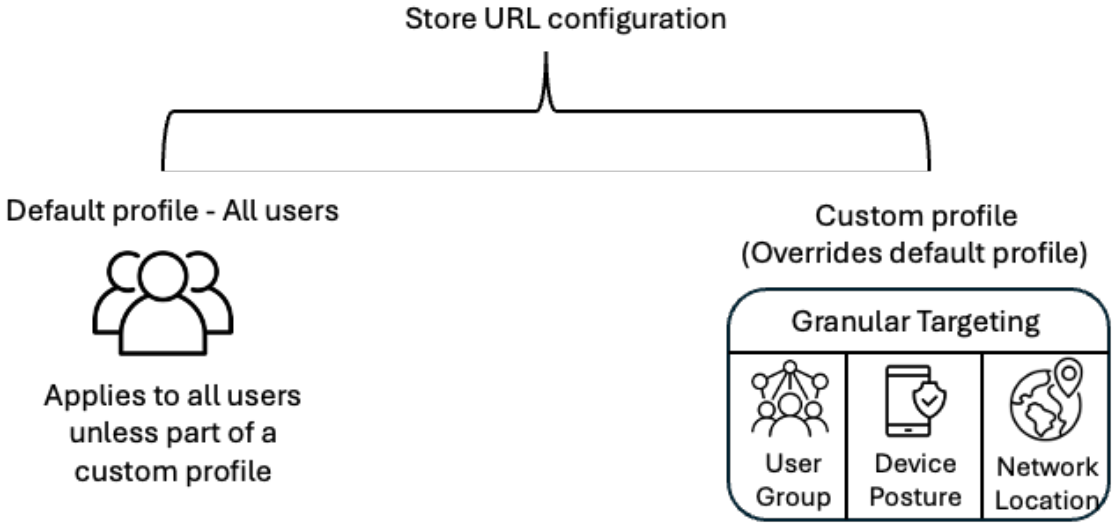
- Default (All users)

  This profile types is the default experience for all users. Settings for default profile apply when:

  - No configuration profile is created for a store URL.
  - The user authenticating to a store does not meet the criteria set for any custom profile.

- Custom profile

  If the user meets the criteria defined by admin in any of the profiles, the client receives settings corresponding to that profile. Settings assigned to a profile are fetched after the user has authenticated to the store.



> **Note:**
>
> Some settings are exclusive to a default profile. If configured, any user who is part of a custom profile inherits the values of such settings. For settings that are configurable via a custom profile, admins need to publish them for the profile for it to be applied.

Profile Limitations

> **Note:**
>
> - You can create up to *20* configuration profiles.
> - You can add up to *10* user groups in a configuration profile.
> - You can add up to *10* device posture tags

> - You can add up to *10* network location tags

Get started with Profiles

September 30, 2025

To get started with this feature, administrators need to review the following support matrix:

Workspace

Citrix Workspace app platform	Minimum supported version	User group rules	Device Posture rules	Network Location rules
Windows	2405	Yes	Yes	Yes
Mac	2405.11	Yes	Yes	Yes

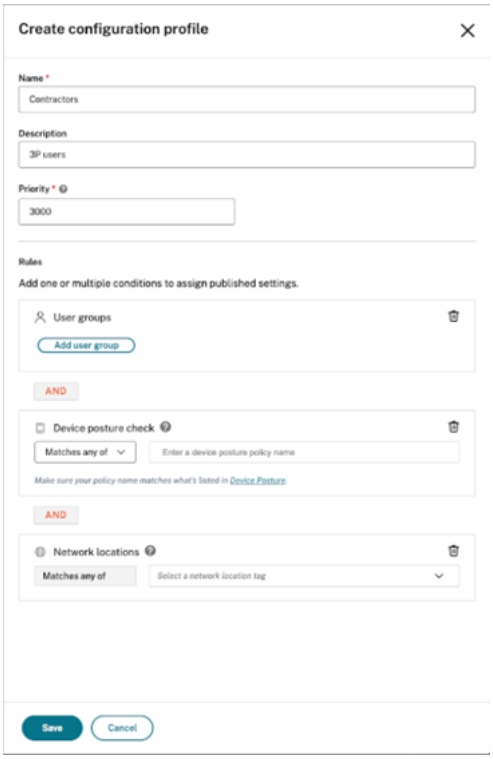
StoreFront

To learn about the prerequisites and how administrators can configure profiles for StoreFront stores, check Setup profiles for StoreFront stores.

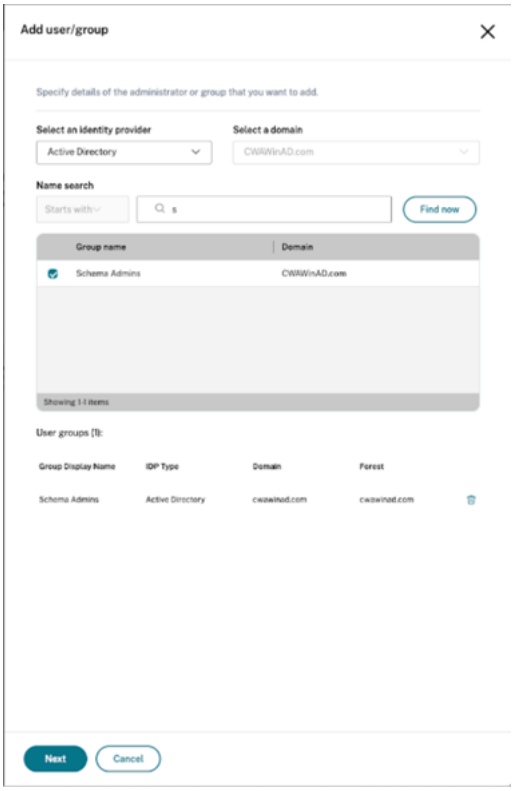
Create a profile

1. Sign in to your **Citrix Cloud** account and navigate to **Client app management**.
2. Under **Stores** section, click **Create profile** to create a configuration profile.
3. Enter the name, description, and priority of the profile in the **Name**, **Description**, and **Priority** fields respectively. To learn more about priority, check Set Priority.
4. In the **Rules** section, you can search for and add **User Groups**, **Device Posture tags**, and **Network Location tags**.

   These entities are combined with a logical AND condition, meaning a user must match all selected criteria to be part of the profile. You can create a profile with a single criteria (for example, only a device posture tag) or a combination of them as required. You can add the desired entities by clicking them from the search list.



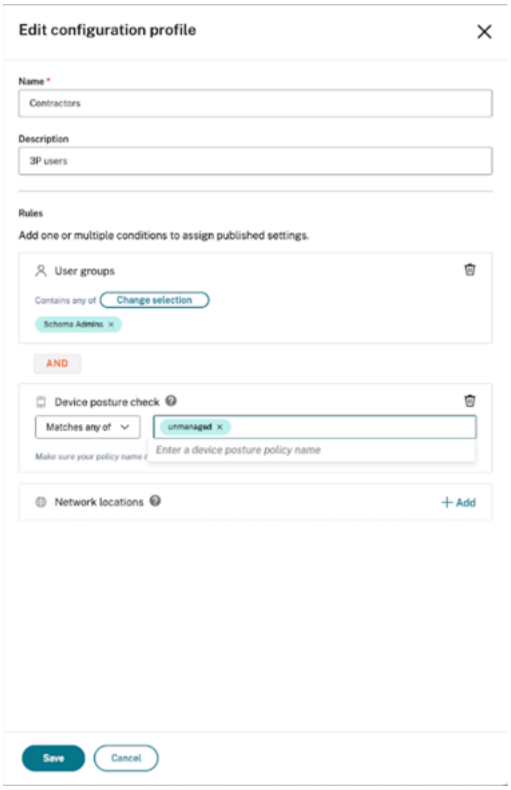
5. To configure user groups, click **Add** option next to **User groups**. In the **Add user/group** workflow, Select an identity provider and a domain name. In the **Name** search field, enter a keyword and search the user groups that you want to add into this profile. Click **Save**.



6. When configuring device posture, the tag must exactly match the policy name created in the device posture section and must be entered as is. If you are adding only the result (for example, `COMPLIANT`, `NON-COMPLIANT`, `DENY`), make sure to enter these tags in uppercase.

   There are three match types used to evaluate device posture when selecting a configuration profile:

   - **MATCHES_ALL:** Device must meet all specified posture requirements.
   - **MATCHES_ANY:** Device must meet at least one specified posture requirement.
   - **DOES_NOT_MATCH:** Device must not meet any of the specified posture requirements.



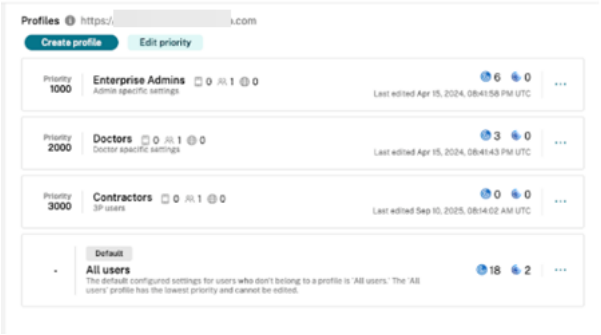
7. When configuring network locations, select the existing tags from the drop-down menu.
8. Click **Save**.

Edit Priority

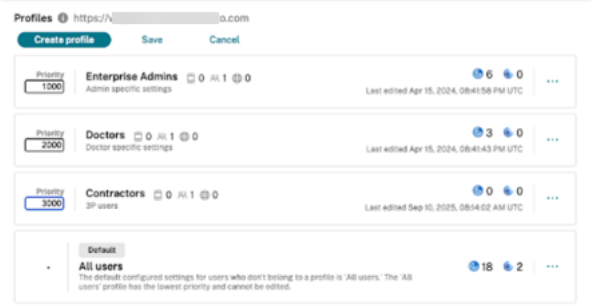
When a user is associated with more than one profile, the system reviews all available profiles against the user's group, device status, and network context. The profile that most closely aligns and has the highest precedence is chosen. **The lower the value, the higher the priority.**

To modify a priority for an existing profile:

1. Select a store URL and click **Edit priority**



2. Edit the number in the **Priority** field. Click **Save**.



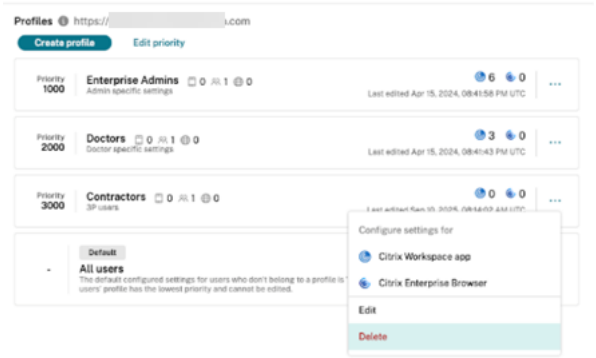
> **Note:**
>
> We recommend leaving sufficient gaps between the priority of configuration profiles, such as 1000, 2000, 3000, and so. This makes it easier to insert new priority values later during the creation of other configuration profiles without needing to edit the existing values.

Delete a profile

To delete a configuration profile, you must reset all configured settings within the configuration profile. The detailed steps are as follows:

1. Navigate to **Client app management** > **Stores**.
2. Select the relevant stores under the **Workspace** or **Storefront** tab.
3. Click the three dots next to the profile that has to be reset for a store URL.
4. Select the relevant app name to go to the settings for that store and profile combination.
5. Go to the three dots as shown after this and click **Reset all**. Provide a confirmation in the follow-up dialog. This deletes all the settings for that profile.

6. Now go to **Stores** and select the same profile. Click **Delete**.



This removes the profile completely for the store URL.

Setup profiles for StoreFront stores

September 30, 2025

Prerequisites

To create profiles for a StoreFront store, the administrators need to meet the following prerequisites:

- Verify Citrix Workspace app version
- StoreFront server requirement
- Configure Cloud Connector or Connector Appliance for Active Directory Management
- Configure registration tool

Verify Citrix Workspace app version

Citrix Workspace app platform	Minimum supported version	User group rules	Device Posture rules	Network Location rules
Windows	2405	Yes	No	No
Mac	2405.11	Yes	No	No

StoreFront server requirement The minimum required version of the **StoreFront server** is **2203.0.3000.14**.

Configure a Cloud Connector or Connector Appliance for Active Directory Management The **Citrix Cloud Connector™** and **Connector Appliance** are Citrix components that serve as a channel for communication between Citrix Cloud and your resource locations. It enables the use of Active Directory forests and domains within resource locations, thereby allowing administrators to access the AD group information for managing configuration profiles.

- To learn more about Citrix Cloud Connector, see Citrix Cloud Connector in the Citrix Cloud product documentation.
- To learn more about Connector Appliance, see Connector Appliance for Cloud Services in the Citrix Cloud product documentation.

Configure registration tool Administrators need to download and run a registration tool on the StoreFront server. The registration tool installs a certificate that establishes trust between the StoreFront server and **Client app management**. As a result, information about the user's AD group can be found and that allows configuration of profiles.

The process involves the following steps:

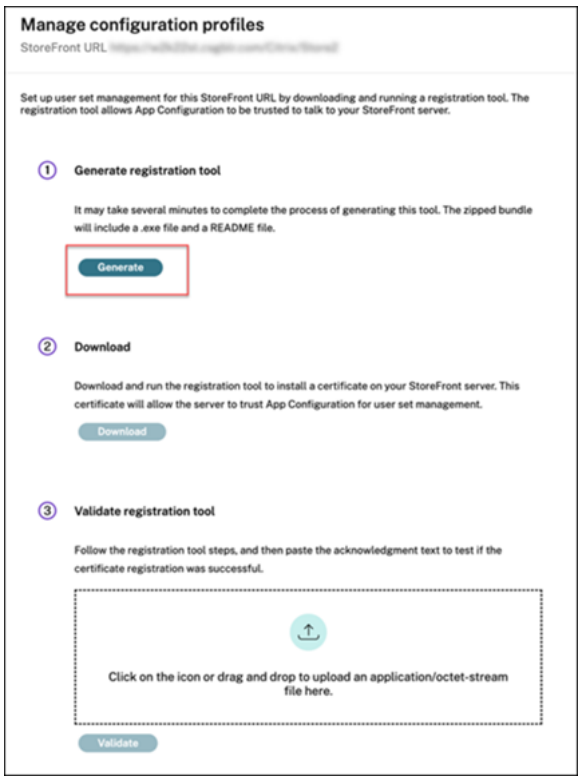
1. Generate a registration tool.
2. Download and run the registration tool.
3. Validate the registration tool.

Generate a registration tool

The registration tool is an executable file that needs to be run on the StoreFront server hosted within the organization. This registers **GACS** as a trusted service to access AD group information.

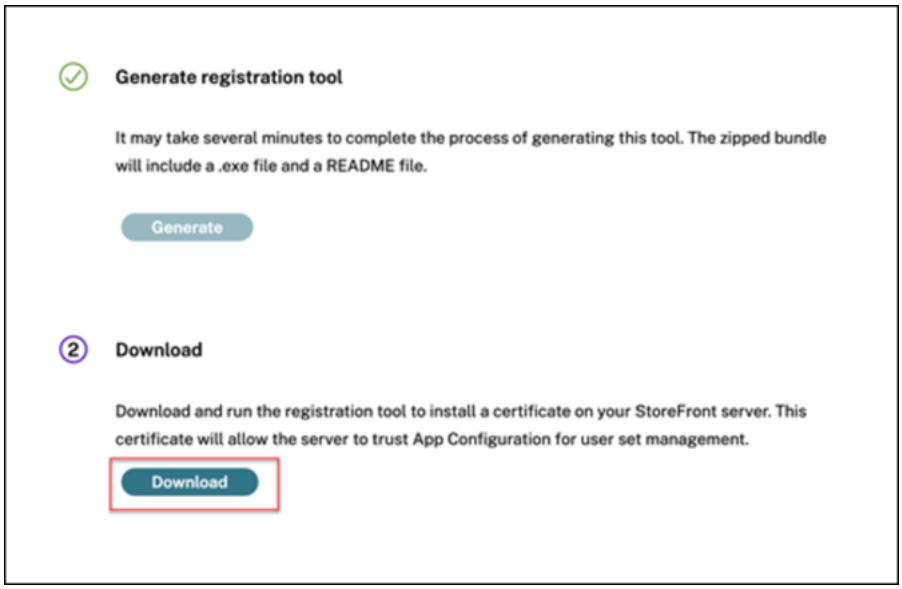
To generate the registration tool, do the following:

1. Navigate to **Client app management** > **Stores**.
2. Select your **StoreFront URL**, and click **Create profile**.
3. On the **Manage configuration profiles** screen, click **Generate** to generate the registration tool.



Download and run the registration tool

Download the registration tool When the registration tool is generated, the **Download** option becomes enabled, allowing the administrator to download the tool. When the administrator clicks the **Download** option, the registration tool is downloaded in an executable format.



> **Note:**
>
> The registration tool is downloaded as a `.zip` file bundled with a README file. The README file provides detailed instructions to download and run the registration tool.

Run the executable file Once the registration tool is downloaded, the administrator can then run the registration tool to install a certificate on the StoreFront server hosted within the organization. This certificate allows the server to trust **GACS** for the configuration Profile Management.

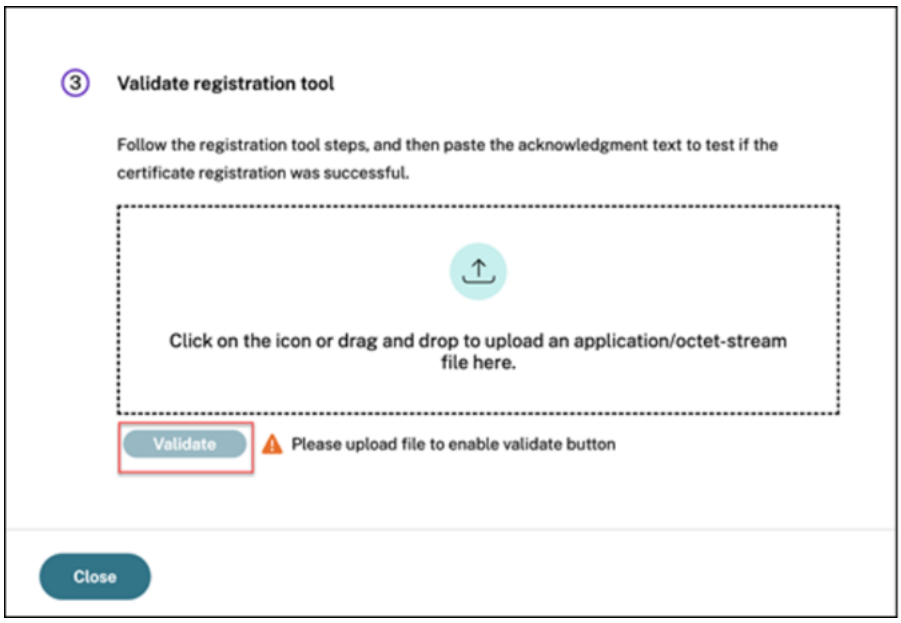
When you run the registration tool, you can decide whether to run the tool on a single store or all stores of the StoreFront server. Once you run the tool, it modifies the `web.config` file of the StoreFront store's authentication service, which registers **GACS** as a trusted service.

> **Note:**
>
> The IIS restarts when the `web.config` file is modified due to the successful execution of the registration tool.

Validate registration tool

Following the successful execution of the registration tool, a `.zip` file is downloaded containing an acknowledgment file and a text file. The text file provides the following information extracted from the StoreFront server:

- **Public Certificate:** The public certificate enables Client app management to process incoming secondary tokens issued by the StoreFront server to provide authenticated, profile-based settings to the client endpoint devices running Citrix applications.
- **Configuration Values:** Various configuration values related to the store are extracted to maintain consistency and ensure that the store operates correctly after any changes or recovery steps.



The administrator has to validate whether the certificate registration is successful by following these steps:

1. Upload the acknowledgment file.
2. Click **Validate**.

   Once the validation of certificate registration is successful, the **Registration validated** message appears.
3. Click the **Close** button.
4. Click **Create Profile** and the **Edit configuration profile** screen appears.

Manage settings for hybrid launch

October 16, 2025

Citrix Workspace app enables its management through Client app management for hybrid launch scenarios.

In a hybrid launch scenario, a user accesses their Citrix resources through a web browser. Upon selecting an app or desktop within the browser interface, the Citrix StoreFront™ server generates an ICA file containing specific instructions for launching that resource. The native Citrix Workspace app reads the ICA file's contents and initiates the connection to the remote application or desktop.

With support for hybrid launch, Client app management now allows you to provide a consistent experience for your users, regardless of whether they access the store through the native app or a browser.

Supported versions of Citrix Workspace app

Citrix Workspace app platform	Minimum supported version
Windows	2503
Mac	2503

Verify the Citrix Workspace app behavior

This section describes Citrix Workspace app behavior in various use cases for hybrid mode.

Scenario	Behavior
A user accesses a store via a web browser and launches a session using client redirection.	The in-session settings apply only from the subsequent launch, while the remaining settings become available for use.
A user adds a store in the app and then accesses the same store via a web browser.	Settings are retrieved and applied through the natively added store.
A user opens a session from Store 1 and then opens another session from Store 2 via a web browser.	The session launched from the most recently accessed store applies its settings.
A user opens a session and Client app management settings are changed during the active session.	Client app management settings are applied during the next session launch.

> **Note:**
>
> Once a session launch is completed, Client app management settings are fetched after the 6-hour time window. If the settings are needed earlier, the user must go to Reset Workspace and launch the session again.

Cloud store support

To get started, administrators need to enable in-memory hybrid launches. This means that you have to disable ICA file download to manage Citrix Workspace app in the case of a hybrid launch. To disable ICA file downloads for Workspace, see Workspace PowerShell documentation.

> **Note:**
>
> Hybrid launch via the Citrix Workspace browser extension isn't currently supported.

On-Premises Support

To get started with this feature, the administrators need to meet the following prerequisites:

- Allow list of Client app management endpoint
- Configure registration tool
- Enable in-memory hybrid launches
- The minimum supported version of StoreFront is 2503.

> **Note:**
>
> Hybrid launch via the Citrix Workspace browser extension isn't currently supported.

Allow list of Client app management endpoint

For more information, see Prerequisites.

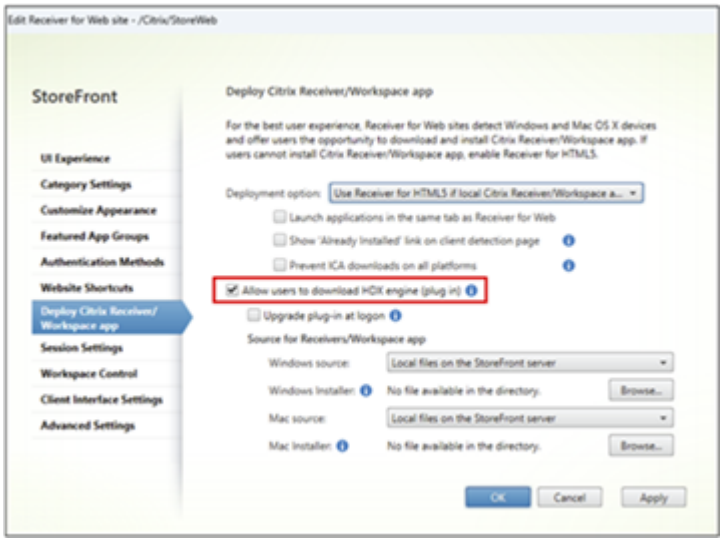
Configure registration tool

For more information, see the Configure registration tool.

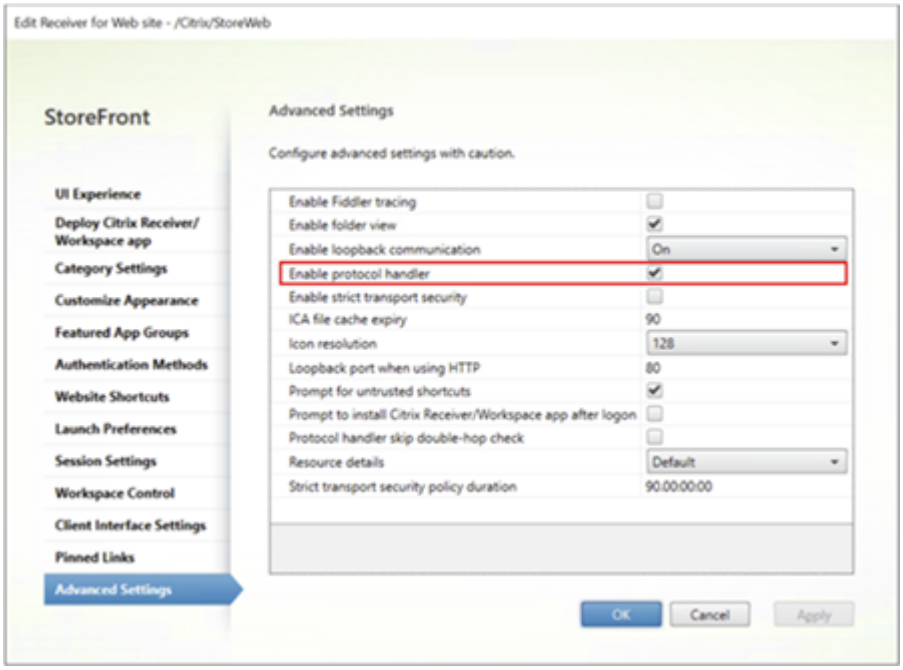
Enable in-memory hybrid launches

To enable in-memory hybrid launches, do the following steps:

1. To allow hybrid launches using Citrix Workspace launcher, select the **Allow users to download HDX™ engine (plug-in)** checkbox.



2. Under **Advanced Settings**, select the **Enable protocol handler** checkbox.



Clone settings across stores, channels, and configuration profiles

September 30, 2025

Clone settings refer to the ability to duplicate settings, which are already configured for an application through Client app management. Instead of going through the entire configuration process again, administrators can simply clone the existing settings to save time and effort. This feature streamlines the workflow, improves productivity, and maintains consistency.

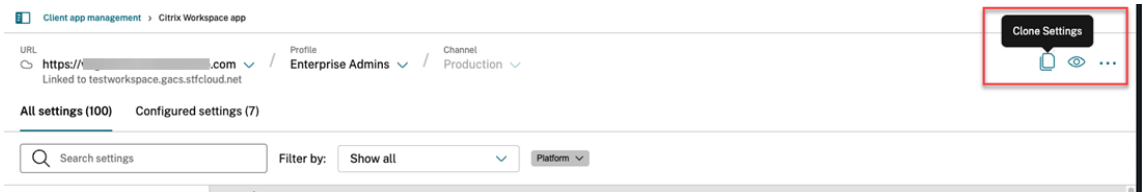
Client app management allows cloning of settings in the following scenarios:

- **Between channels:** Clone the configured settings from one channel to the other.
- **Between profiles:** Clone the configured settings between configuration profiles created within the store.
- **From store to a profile:** Clone the configured settings in default profile (all users) to a configuration profile.
- **Between stores:** Clone the configured settings from the current store to another store.

> **Notes:**
>
> - Cloned settings overwrite the existing settings at the destination.
> - Settings that are exclusive to a default profile can't be cloned to the configuration profile with "From store to a profile"clone option.
> - Cloning between stores is possible only with stores of the same type. Both the source and destination stores must be either Workspace stores or StoreFront™ stores.

To use this feature, you need to:

1. Navigate to **Client app management** > **Stores**.
2. From the list of configured store URLs, select the store for which you want to map settings and then click **Configure**.
3. Select the desired store from the given store list, and click the **Clone Settings** option.

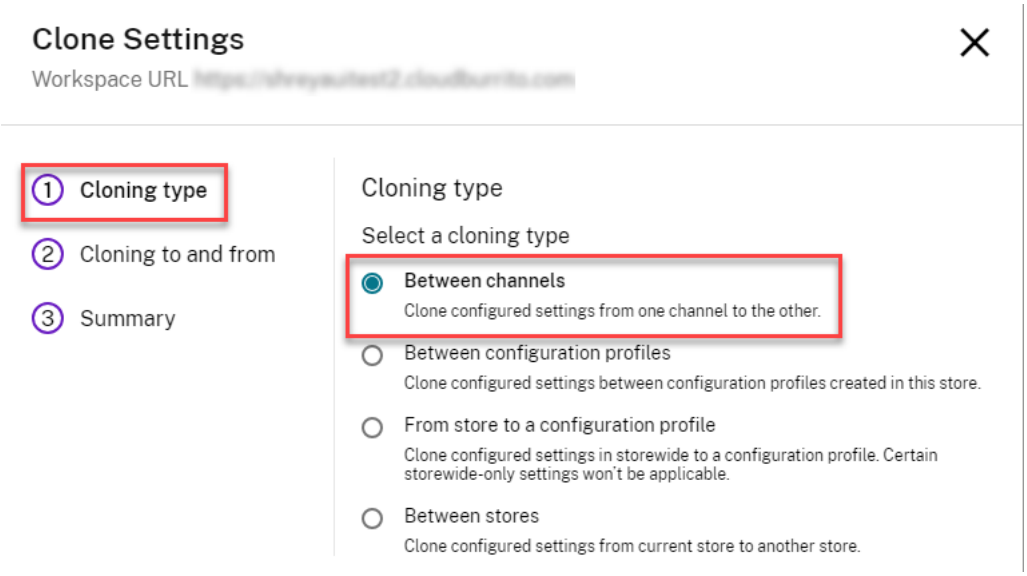


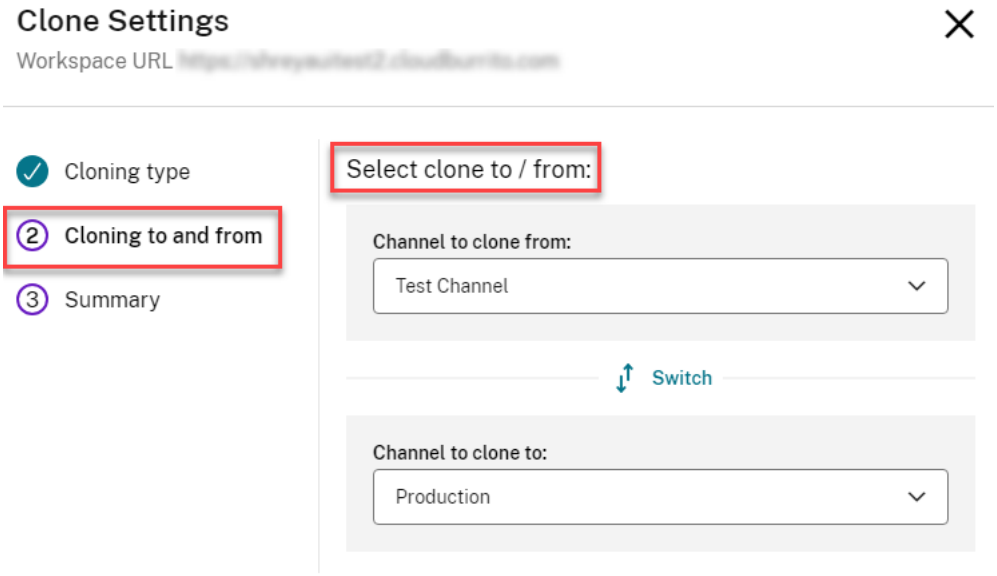
4. Select a cloning type from the **Clone Settings** window and click **Next**.
5. Select **Cloning to** and **from** information by selecting the appropriate details from the drop-down list.

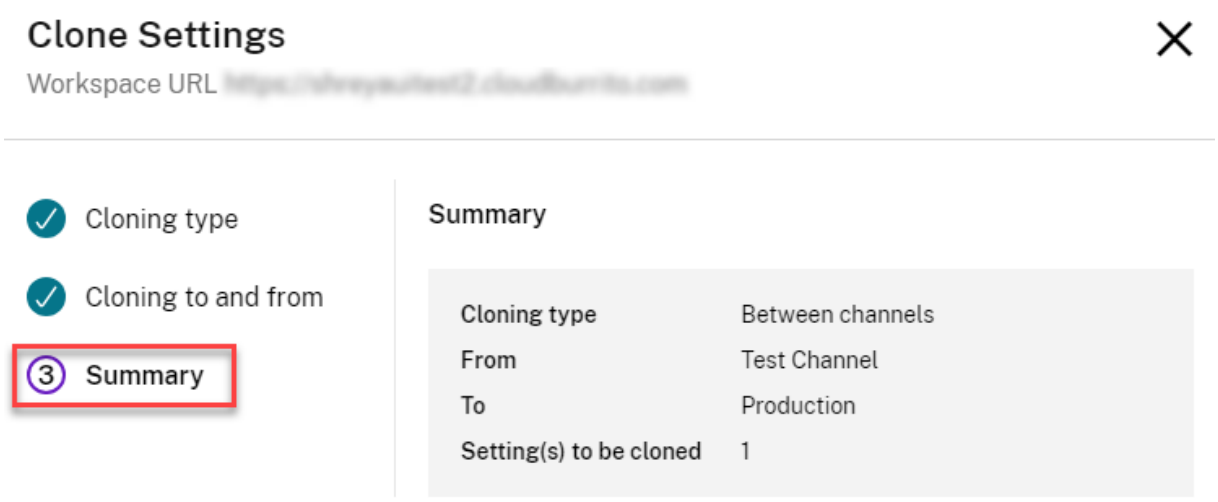
See the following sections for more information about steps 4 and 5.

Clone settings between channels

You can clone the settings between Production and Test Channel in Storewide.

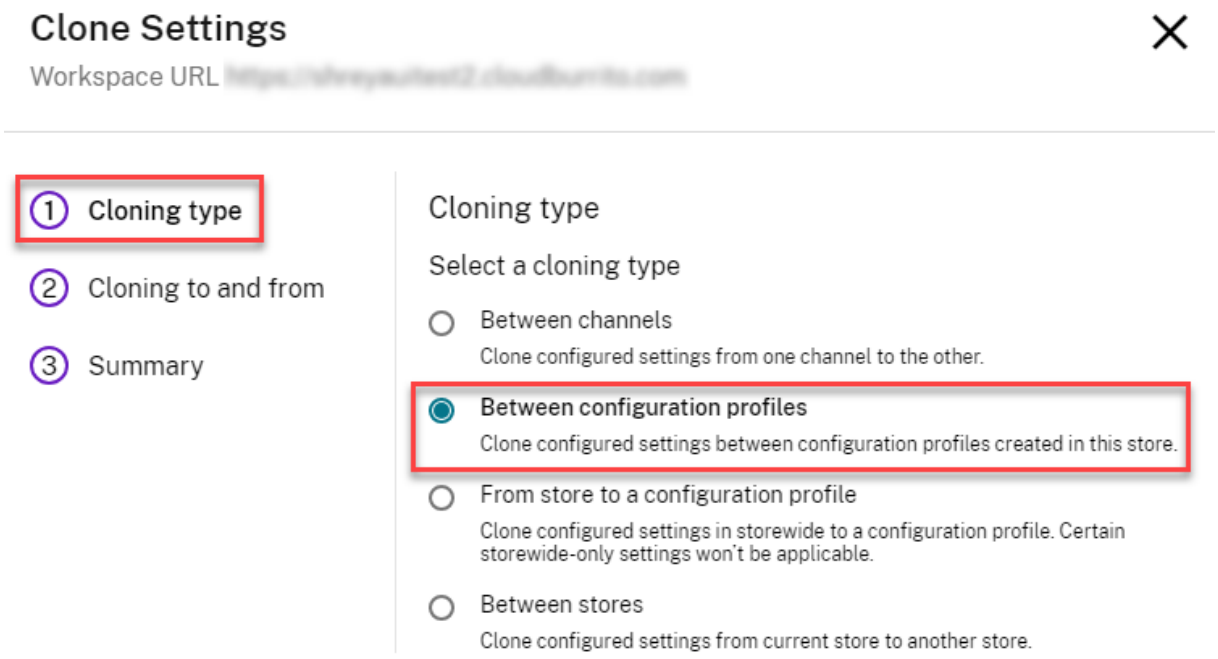


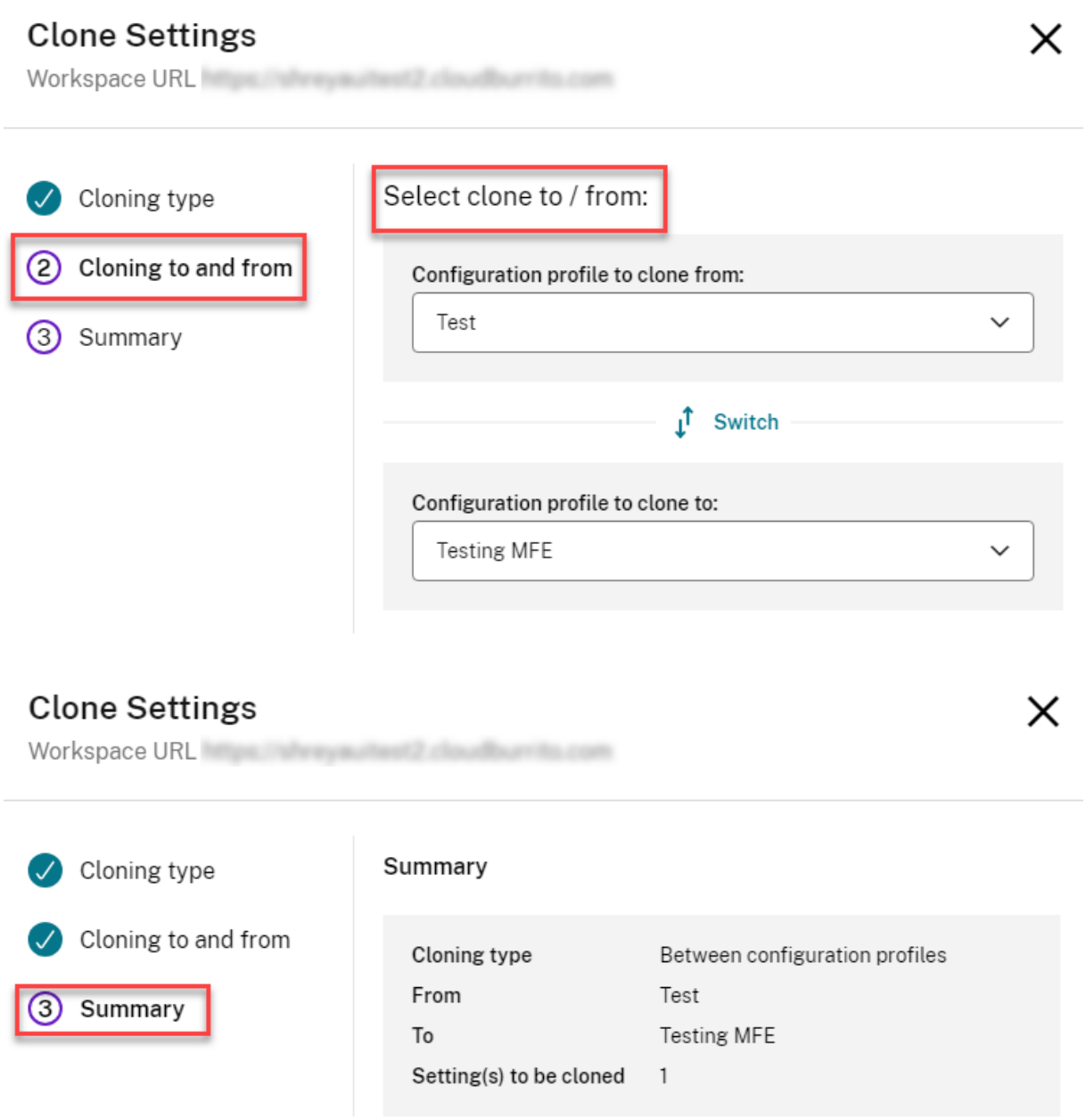




Clone settings between configuration profiles

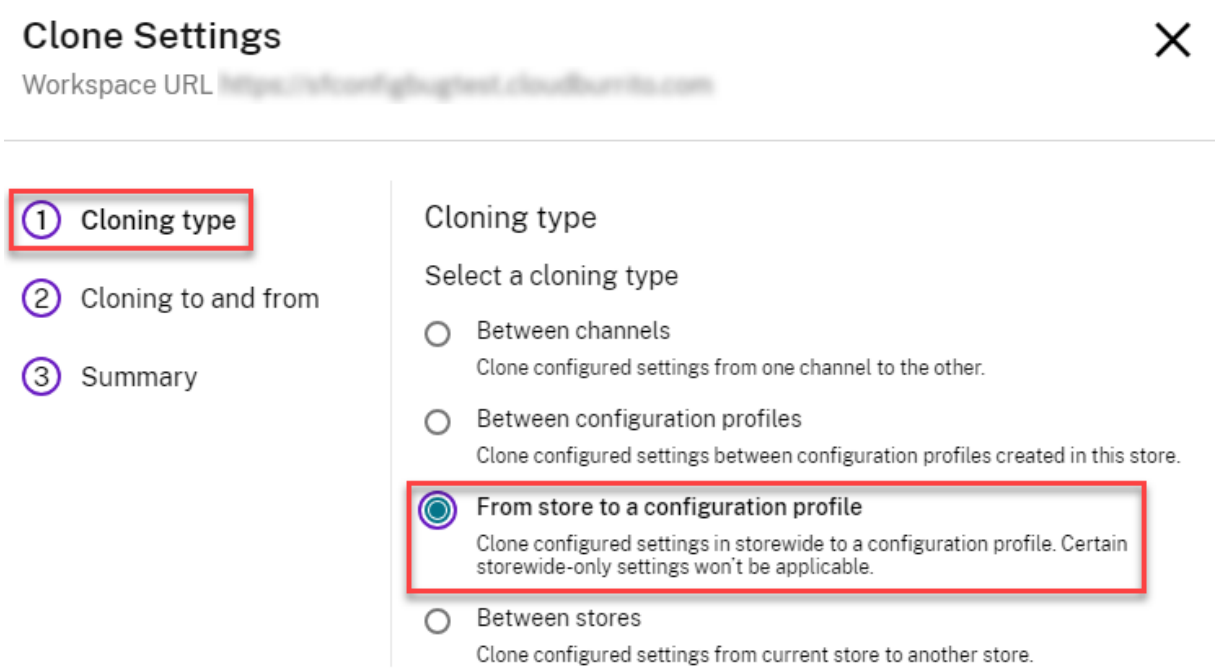
You can clone the settings between two configuration profiles.

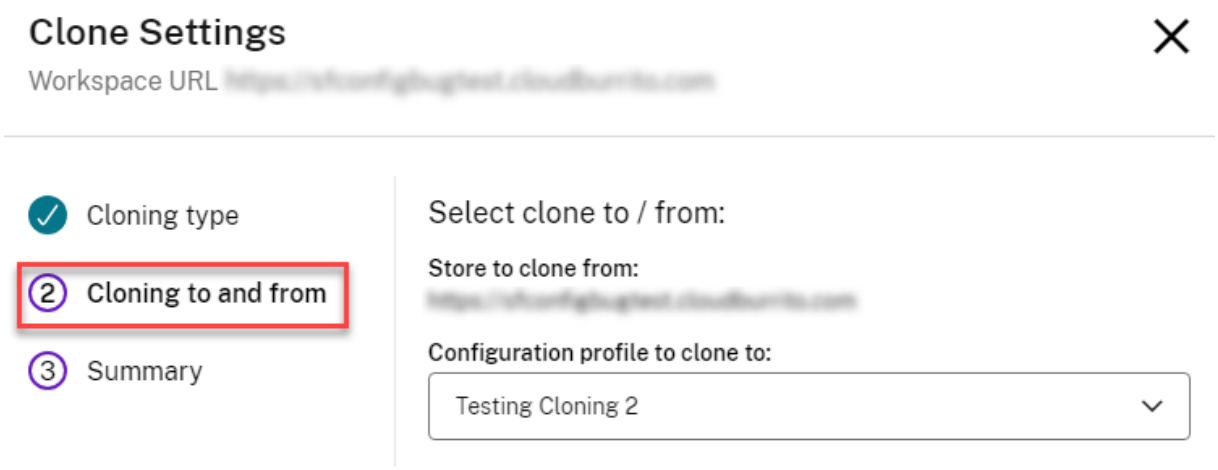


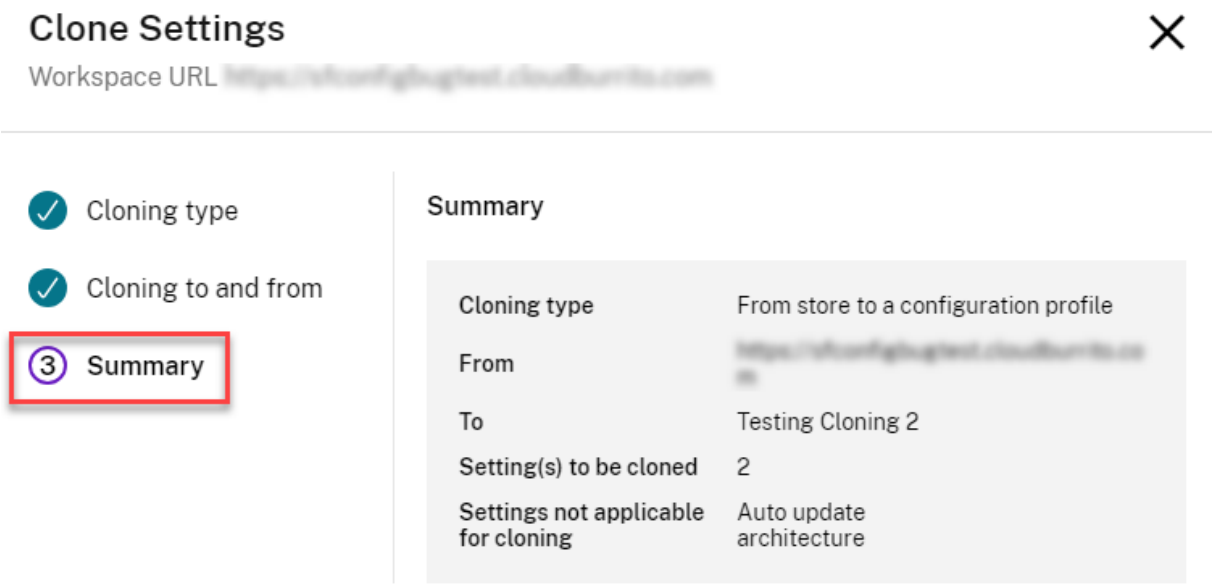


Clone settings from store to configuration profiles

You can clone the settings from a store to a configuration profile.

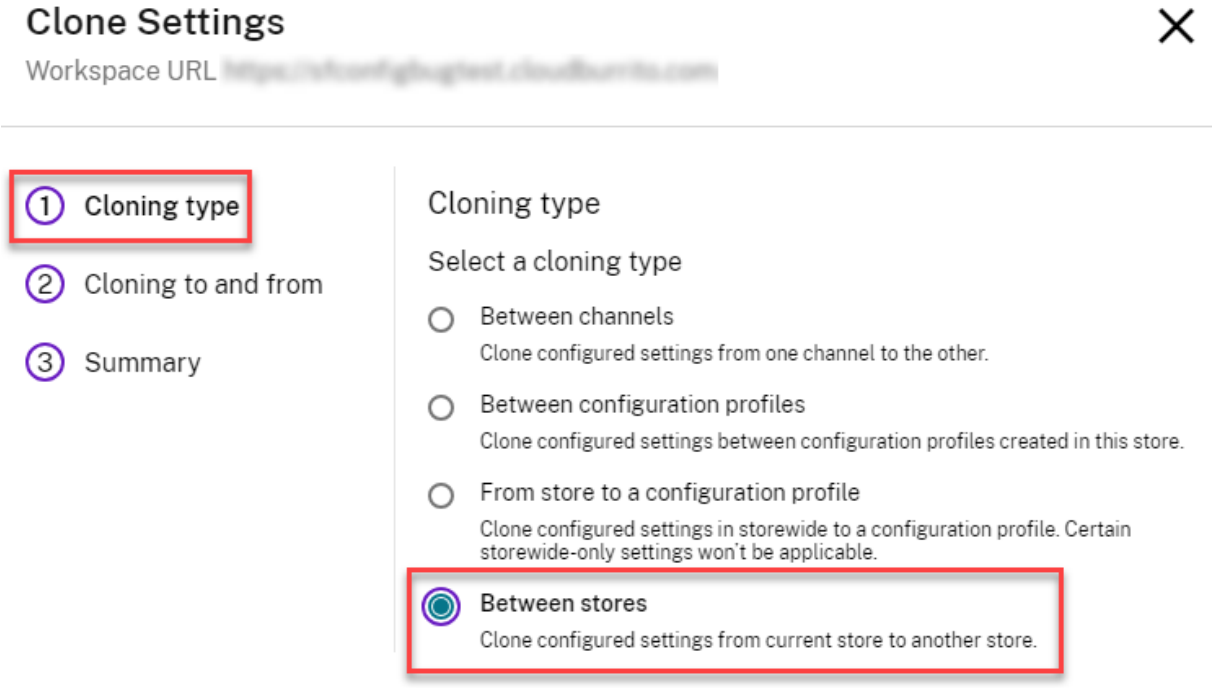


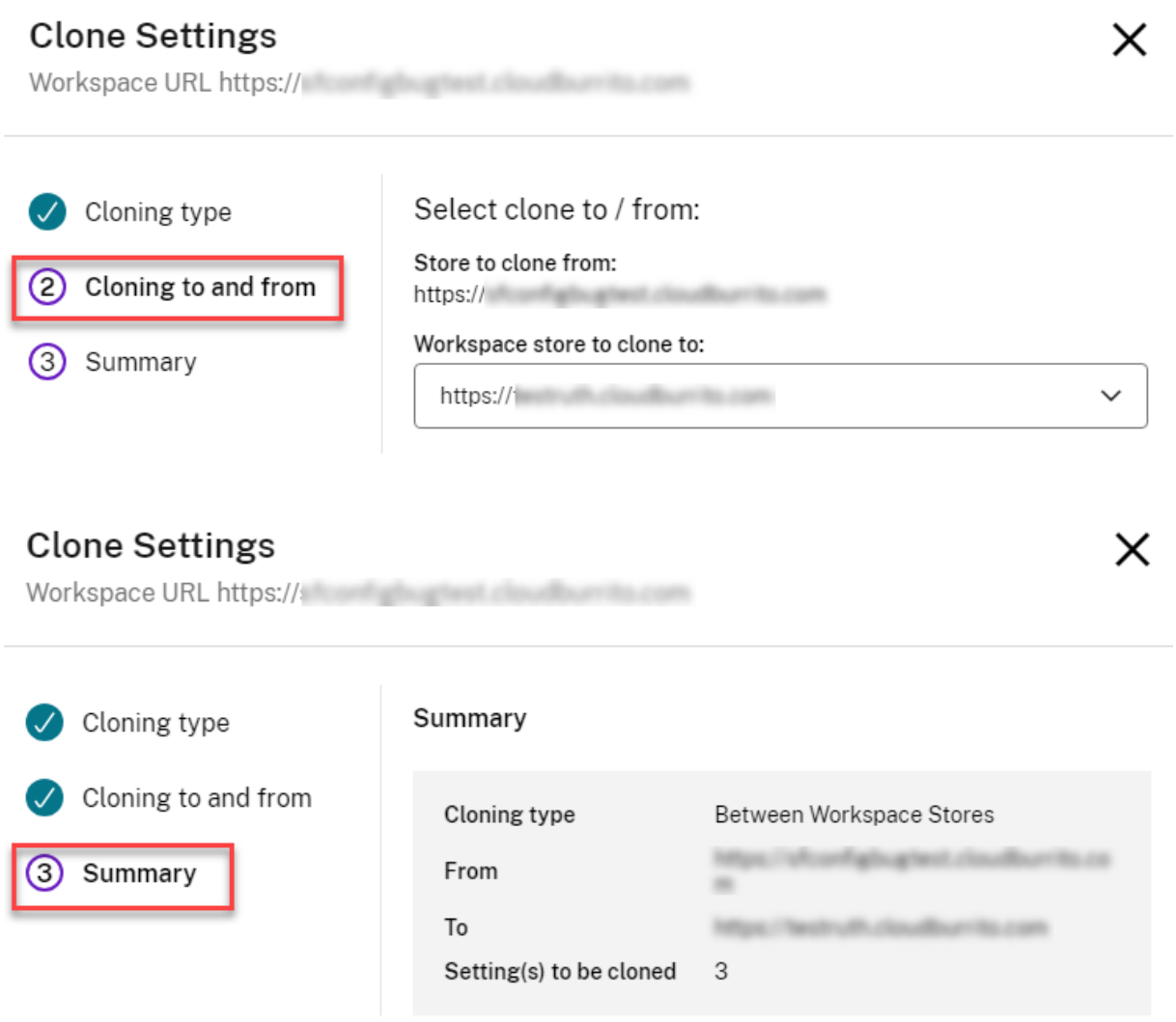




Clone settings between stores

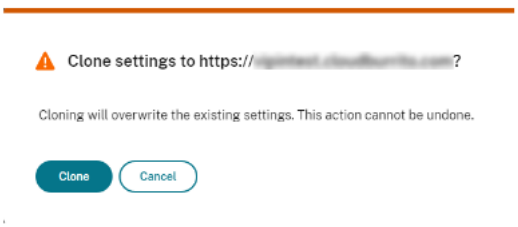
You can clone the settings between stores.



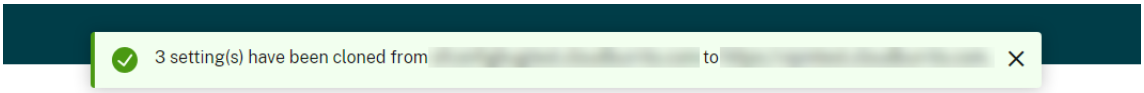


After selecting the cloning options:

1. Click **Next**.
2. Verify the configured clone settings on the **Summary** page, and click **Clone**.



You can see a notification following the successful cloning.



Client app considerations

September 30, 2025

Administrators use the Client app management to publish settings associated with their StoreFront or Workspace or Gateway URLs. Supported Citrix clients are built to interact with this service. This section outlines the key considerations and best practices to allow Citrix client apps to work with Client app management.

Discovery of a newly managed store

If an administrator has published settings for a Store URL for the first time, the client apps accessing that store needs to discover it has to pull settings from Client app management.

The discovery happens on the following basis:

- **New store addition**: If a user is adding a store to the client for the first time, discovery is immediate
- **Already added store**: For an already added store, the client has a 24-hour cadence to check if the store has settings configured via Client app management.

If an immediate discovery is needed for a store, click the **Accounts** icon within Citrix Workspace app and then click **Refresh**.

For a discovered store, the cadence for setting pull is shared as follows.

Frequency of fetching updated settings

For an already configured store, Citrix client apps pull settings on the following basis:

1. **New store addition**: Occurs when the store is added.
2. **Already added store**: The settings are fetched as per the following cadence:

Platform	Maximum time required to update settings
Citrix Workspace app for Windows	• 6 hours for 2503.1 and older versions • 30 minutes for 2507 LTSR and newer versions
Citrix Workspace app for Mac	• 6 hours for 2505.10 and older versions • 30 minutes for 2508 and newer versions
Citrix Workspace app for Linux	6 hours
Citrix Workspace app for ChromeOS	3 hours
Citrix Workspace app for HTML5	3 hours
Citrix Workspace app for iOS	6 hours
Citrix Workspace app for Android	6 hours

Order of precedence for application of settings

In addition to the Client app management, there are platform-specific Endpoint Management solutions that can be used to configure end-user settings. In the event of a conflict between settings configured through the Client app management and other platform tools, the settings are applied in the following order.

Platform	Store type	Order of precedence
Citrix Workspace app for Windows	StoreFront and Workspace	Group Policy Object (GPO)/ **Device management solution** > **Client app management**
Citrix Workspace app for Mac	StoreFront and Workspace	**Device management solution** > **Client app management** > **UserDefaults**
Citrix Workspace app for Linux	Workspace	**Device management solution** > **Client app management**
Citrix Workspace app for HTML5	StoreFront	**Client app management** > **Configuration.js**
	Workspace	Client app management

Platform	Store type	Order of precedence
Citrix Workspace app for ChromeOS	StoreFront	**Google Admin Policy** > **Client app management** > **Configuration.js**
	Workspace	**Google Admin Policy** > **Client app management**
Citrix Workspace app for iOS	StoreFront and Workspace	**Mobile Device Management (MDM)** > **Client app management**
Citrix Workspace app for Android	StoreFront and Workspace	**Mobile Device Management (MDM)** > **Client app management**

Citrix Workspace app

October 17, 2025

Administrators can control Citrix Workspace app settings for users who access their store through two primary methods:

1. **Directly via Citrix Workspace app**: Users with compatible Citrix Workspace app versions access their workspace directly through the native application.

   Supported versions for Citrix Workspace app

Citrix Workspace app platform	Minimum supported version
Windows	Current Release - 2106, LTSR - 2203.1
Mac	2203.1
Linux	2408
iOS	2104
HTML5	2111
ChromeOS	2203
Android	2104

2. **Hybrid Launch**: Users access their Workspace URL through a web browser. Launching virtual desktops and apps requires a compatible version of the Citrix Workspace app client to be installed locally.

Support versions of Citrix Workspace app for Hybrid Launch:

Platform	Windows	Mac	ChromeOS	HTML5	Android	iOS	Linux
Support available	Yes	Yes	No	NA	No	No	No
Version support	2503	2503	NA	NA	NA	NA	NA

Managing Citrix Workspace app rollout

October 17, 2025

Start with the default behavior around auto update and then dive into options with Client app management.

Use the **Updates and Plugins** category of **Client app management** to specify which Citrix Workspace app version your end users must use for optimal results.

You can set up a rule to:

- Update the app to the latest CR (Current Release) or LTSR(Long Term Service Release) version.
- Update the app to a specific CR (Current Release) or LTSR(Long Term Service Release) version.
- Trigger the auto update within a determined rollout period.
- Trigger the auto update within a specific time of the day.

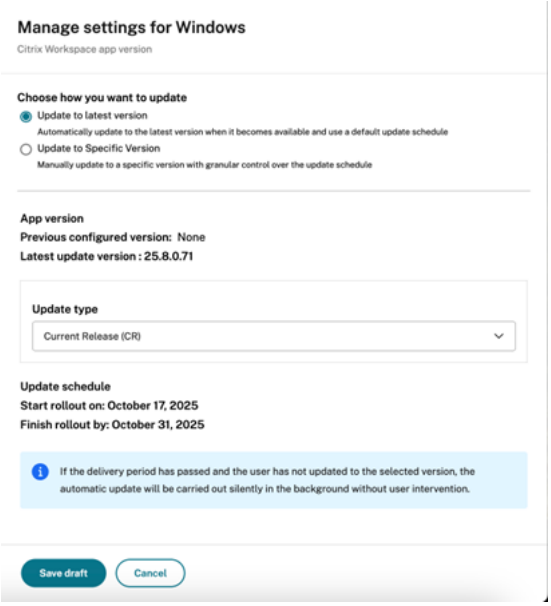
> **Note**:
>
> This setting can be configured only for macOS and Windows OS.

Update the app to the latest CR or LTSR version

To manage the app version settings:

1. Sign in to your Citrix Cloud console.
2. Navigate to **Client app management** > **Citrix Workspace** > **Updates and Plug-ins** category.

3. Expand the **Citrix Workspace app Version** setting.
4. Select **Windows** or **Mac** checkbox and then click **Edit**.
5. If you select the **Update to latest version**, you can choose between Current Release(CR) or Long Term Service Release(LTSR). The upgrade happens as per the Citrix-determined update schedule. If the delivery period has crossed, the upgrade is carried out during the next auto update cycle of the specific client.

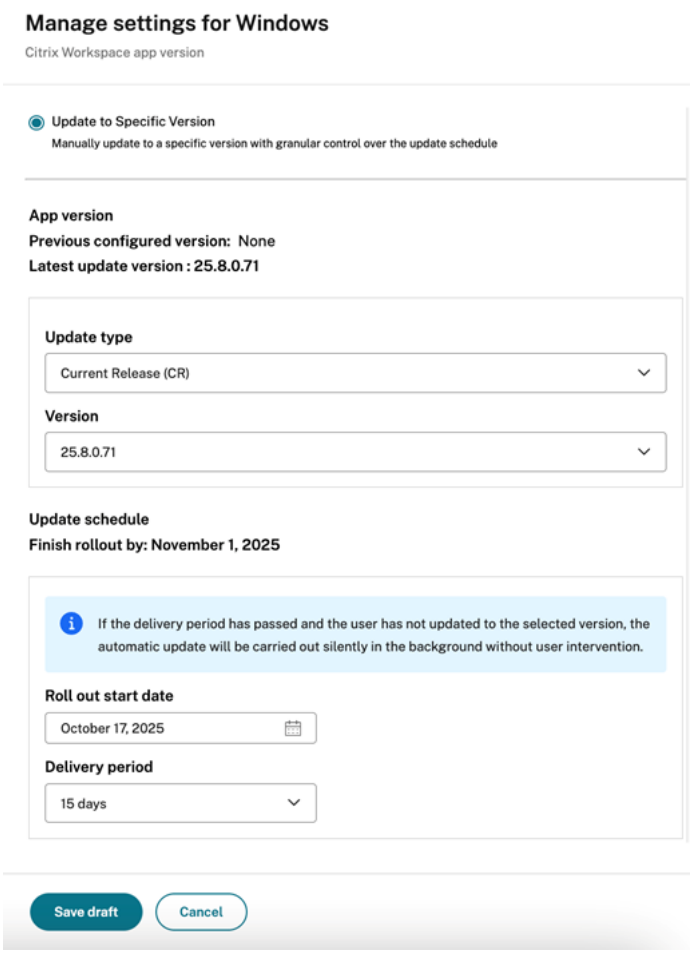


6. Save your settings and publish them.

Update the app to a specific CR or LTSR version

1. Navigate to **Client app management** > **Citrix Workspace** > **Updates and Plug-ins** category > **Citrix Workspace app Version**.
2. Select **Windows** or **Mac** checkbox and then click **Edit**.
3. Choose the following. If you select **Update to Specific Version**, you can choose between:

   - **Update type**: Current Release(CR) or Long Term Service Release(LTSR).
   - **Version**: Define the Citrix Workspace version that you want to allow for the automatic update.
   - **Roll out start date**: Define the start date at which you prefer to start the automatic update of your Citrix Workspace app.
   - **Delivery period**: Enter the number of days up to which the automatic update rolls out. The automatic update process completes within the specified delivery period. The delivery period is an increment of 5

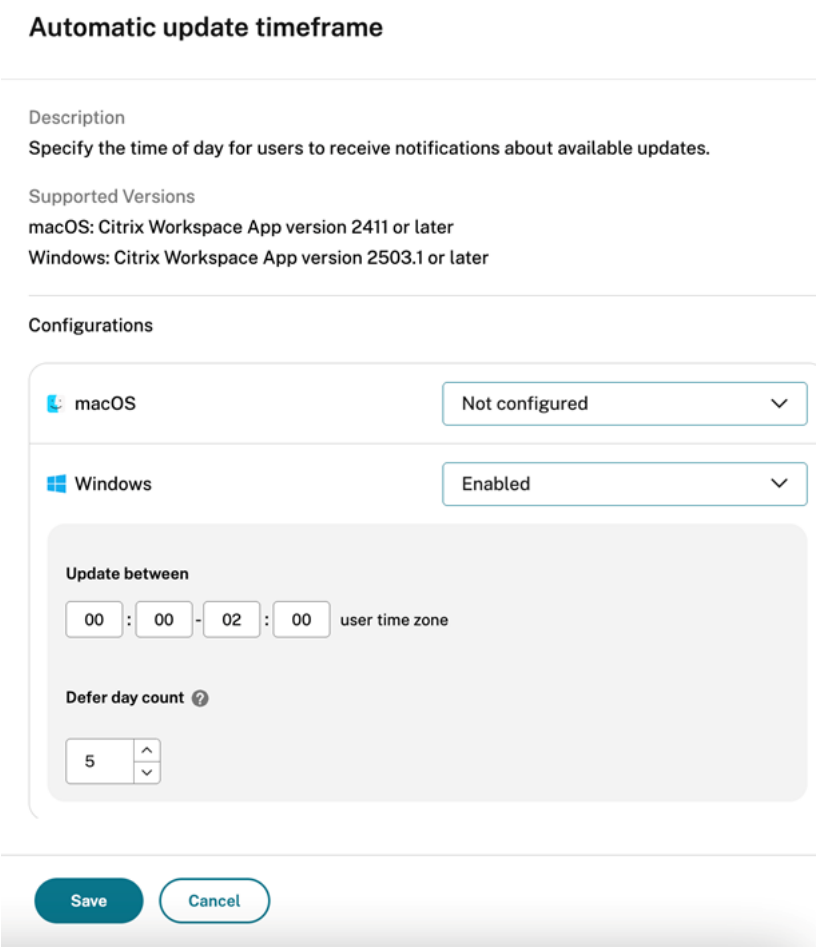


4. Save the settings.

> **Note**:
>
> Once the delivery period expires, Citrix Workspace app automatically updates at the next available opportunity.

Triggers the auto update within a specific time of the day

Administrators can now schedule automatic updates for Citrix products at any preferred time on their Mac devices. During this specified time, software updates automatically or users receive notifications on available updates. The aim is to minimize disruption to end users during their working hours, thereby providing an enhanced user experience.



To enable this feature, do the following:

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

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

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

- **Defer day count**: In this field, mention the number of times users can postpone the automatic update. When a user runs out of the allocated defer count, the automatic update occurs during the time frame defined in the **Update between** fields.

Manage plug-ins for Citrix Workspace app

October 17, 2025

With Client app management, you have a centralized platform to install and update plug-ins across managed and personal devices. Either Citrix or its partners must build these plug-ins.

> **Note**
>
> Plug-in installation or upgrade is supported on the following Citrix Workspace app versions:
>
> - Citrix Workspace app for Windows 2212 (Current Release) or later
> - Citrix Workspace app for Windows 2402 (LTSR)
> - Citrix Workspace app for Mac 2409 or later

If your store is configured through Client app management and end users have already added that store to their Citrix Workspace app, any change in the plug-in setting is reflected as per the duration specified here. This means that after you publish your changes, it might take a few hours for the settings to be updated on the client side, depending on the platform.

After the configuration has been fetched on the Citrix Workspace app, the Citrix Auto-Update service installs the plug-in as per your **Automatic Update Timeframe** settings or within 24 hours, whichever is sooner.

> **Note:**
>
> End users can manually update to the latest version of the plug-ins using the Check for updates option in their system tray. This overrides any delay group settings. However, this option also updates the Citrix Workspace app, either to the latest version or to the version specified by the admins.

Supported plug-ins can be found under the **Updates and plug-ins** section of Citrix Workspace app on the Client app management. The supported plug-ins include:

- Endpoint Analysis
- Citrix Secure Access
- Webex VDI plug-in Installer Engine
- Zoom VDI plug-in Management
- Microsoft Teams VDI plug-in
- ControlUp RemoteDX plug-in Management

Citrix Endpoint Analysis plug-in

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

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

You can configure your plug-in settings as described in the Deployment mode settings section.

> **Note**:
>
> This plug-in is available only on Windows and Mac platforms.

For more information, see Manage Citrix Endpoint Analysis client for Device Posture service.

Citrix Secure Access Agent

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

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

You can configure your plug-in settings as described in the Deployment mode settings section.

Webex VDI Plug-in Installer Engine

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

> **Notes:**
>
> - This plug-in is available only on the Windows platform.
> - The Webex VDI plug-in installer engine is installed during the regular auto update of the Citrix Workspace app or when you check for updates manually.

Important: Citrix only manages the installation and update of the Webex VDI Plug-in manager. The Webex plug-in that is installed on the end-user's device is managed by Webex itself.

Configure plug-in settings

Before proceeding, you must ensure that you've completed the steps listed in the following Prerequisites section. You can then configure your plug-in settings as described in the Deployment mode section.

Prerequisites The following steps must be followed for configuring the Virtual Channel:

1. Either disable or configure the Virtual Channel List policy on the Broker to allow Webex to use the VC as documented here.
2. Enable Auto upgrade for the VDI plug-in on the Virtual Desktop where the Webex App for VDI is installed using the following registry key

`HKEY_LOCAL_MACHINE\SOFTWARE\Cisco Spark Native, set AutoUpgradeVDIPluginEnable=1`

You can now sign in to your Citrix Cloud account and configure your plug-in settings as described in the Deployment mode settings section.

Webex VDI plug-in compatibility with Webex app

After the configuration is done, a refresh option appears in the menu on the Webex app running in the VDI. Click the refresh option, the Webex app closes, and the Webex VDI plug-in is installed on the user's endpoint.

The Webex VDI plug-in does not appear in the list of programs on Windows even after installation. To check if the plug-in is installed, you can run a **Health Check** on the Webex app running in the VDI. Check the **VDI** section to verify if the plug-in is installed. You can also verify if the plug-in version is compatible with the Webex app version.

The Webex VDI Plug-in Installer Engine automatically installs the latest Webex plug-in version, which is compatible with the end user's Webex app. For more information on compatible versions, refer to Webex Version support.

If the versions don't match, check if you've disabled the Compatibility check on the VDI using the following steps:

1. Go to `HKEY_LOCAL_MACHINE\Software\Cisco Spark Native\`.
2. Create a DWORD (32-bit) registry key named **VDIDisableCompatibilityVersionCheck** and give it one of these values:

- 0—enables the version compatibility check (default)
- 1—disables the version compatibility check

Zoom VDI Plug-in Management

With GACS, you can manage the Zoom VDI Plug-in manager. The Zoom VDI Plug-in manager, in turn, installs and manages the Zoom plug-in installed on the end-user's device.

> **Important**:
>
> Citrix only manages the installation and update of the Zoom VDI Plug-in manager. The Zoom plug-in that is installed on the end-user's device is managed by Zoom itself.

Configure plug-in settings

Before proceeding, you must ensure that you've completed the steps listed in the following Prerequisites section. You can then configure your plug-in settings as described in the Deployment mode settings section.

Prerequisites The following steps must be followed for configuring the Virtual Channel:

1. Either disable or configure the Virtual Channel List policy on the Broker to allow Zoom to use the Virtual Channel as documented here.
2. Enable the virtual desktop for Zoom VDI plug-in Management with registry key as documented here.

You can configure your plug-in settings as described in the Deployment mode settings section.

Once the configurations are done, open the Zoom app and keep it running on the VDI. The user must see a pop-up (prompt) after sometime (once the Zoom VDI plug-in installer is downloaded on the user's endpoint) letting them know that the session disconnects to install the VDI plug-in on the endpoint. Upon clicking **OK**, Zoom might close the Citrix Session and proceed to install the plug-in on the user's endpoint.

Microsoft Teams VDI Plug-in Management

The Microsoft Teams VDI Plug-in Manager optimizes the audio and video for calls and meetings. With the Global App Configuration service, you can manage the installation of Microsoft Teams Plug-in Manager. This Plug-in Manager, in turn, installs and manages the Microsoft Teams Optimization plug-in (VDI 2.0 or SlimCore engine) on the end-user's device.

Configure plug-in settings

Before proceeding, you must ensure that you've completed the steps listed in the following **Prerequisites** section.

Prerequisites Administrators are required to configure a new registry setting in the VDA to enable the new Microsoft Teams to access the Citrix virtual channel. For more information, see the **Note** given in Optimization for Microsoft Teams. This registry setting is not required if you're using Citrix Virtual Apps and Desktops 2402 LTSR and above (or) 2203 LTSR CU5 and above.

You can now sign in to your Citrix Cloud account and configure your plug-in settings as described in the Deployment mode settings section.

For more information, see New VDI solution for Microsoft Teams.

> **Notes**:
>
> - Reconnect the session after the successful installation of the plug-in on the end-user device. After that, the Microsoft Teams VDI app must be restarted twice to enter VDI 2.0 mode.
> - This plug-in is available only on the Windows platform, and it is applicable starting with Citrix Workspace app for Windows version 2405.
> - This plug-in is only applicable to New Microsoft Teams (Microsoft Teams 2.x) and not Classic Microsoft Teams.

ControlUp's RemoteDX Plug-in Management

ControlUp's RemoteDX is a monitoring and troubleshooting solution designed to improve the end-user experience for remote workers. The key features include Endpoint Monitoring, Network Insights, Session Visibility, and Proactive Alerts. With the Global App Configuration service, you can manage the ControlUp's RemoteDX Plug-in manager.

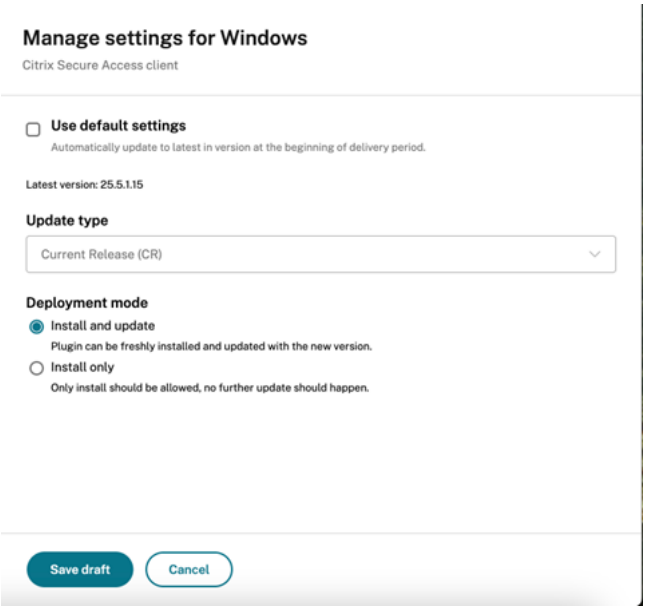
> **Important**:
>
> Citrix only manages the installation and update of the RemoteDX Plug-in manager. ControlUp directly manages the RemoteDx plug-in installed on the end-user's device. ControlUp also manages any telemetry data collection by the RemoteDX plug-in from an end-user's device.

Deployment mode settings

Sign in to your Citrix Cloud account and navigate to **Workspace Configuration** > **App Configuration**. From the list of configured URLs, select the one for which you want to map settings, and click **Configure**. Under the **Updates and Plug-ins** section, navigate to the desired plug-in and click the expanded icon to view the applicable platforms. Select the platform that you want to configure the settings for and click **Edit**.

- **Install and update**: Installs the latest version of the plug-in on the end-user's device. It automatically updates the plug-in to the latest version.

- **Install only**: Installs the latest version of the plug-in on the end-user's device. It does not auto-update.



Email based discovery

September 30, 2025

An email based discovery service allows end users to sign in automatically to the store on their Citrix Workspace™ app using their email addresses. Thus, users don't need to enter their store URLs.

Setup email based discovery for cloud stores

To enable email-based discovery for cloud stores, do the following steps:

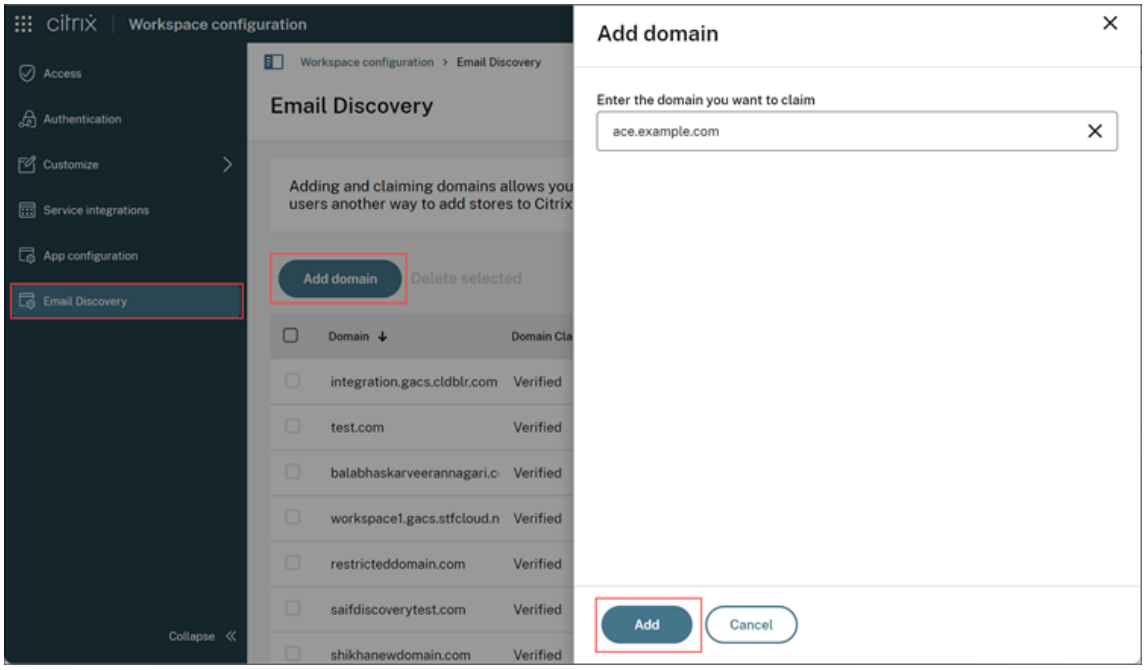
1. Claim a domain
2. Create a domain to URL mapping

Claim a domain

To claim a domain:

1. Sign in to Citrix Cloud.
2. Navigate to **Workspace configuration** > **Email Discovery**.

3. Click **Add Domain**.
4. Enter the domain that you want to claim (For example, `ace.example.com`).

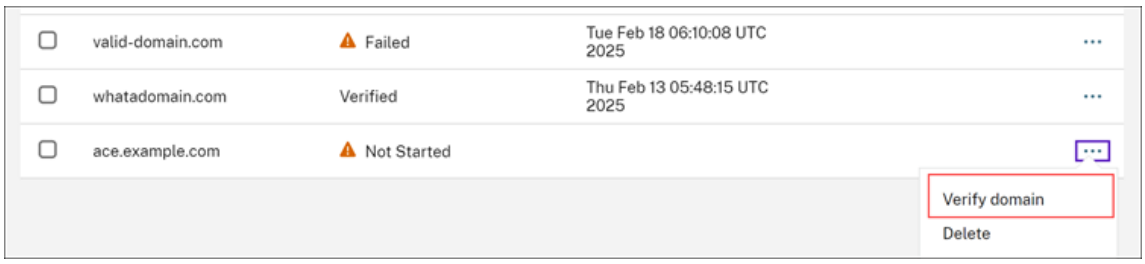


5. Click **Add**.

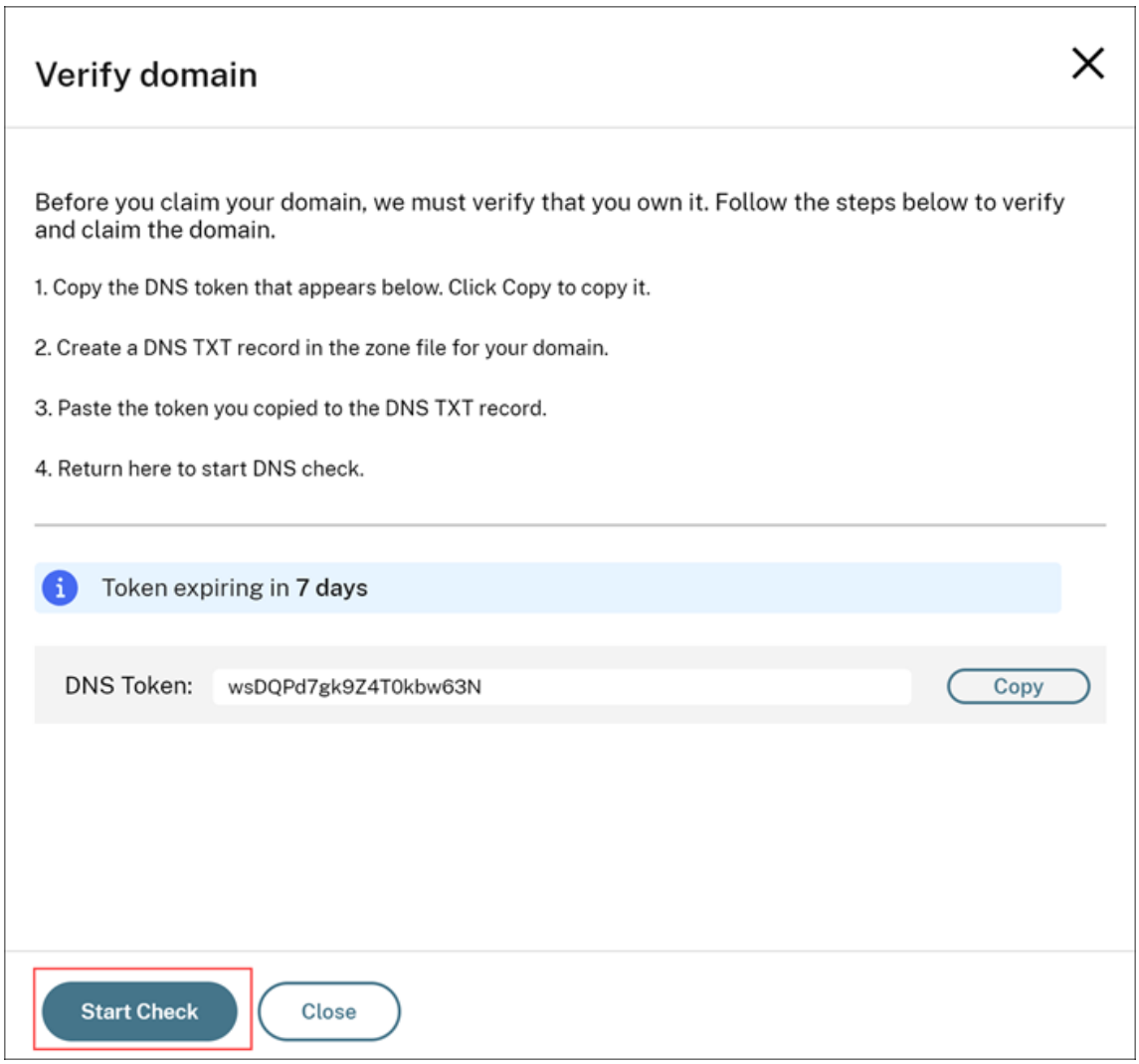
   You can see that the domain is added on the **Email Discovery** page.

   The domain claim status is shown as **Not Started**. You must verify the domain as shown in the following steps:

6. Click the ellipsis menu (**...**), and then select **Verify domain**.



7. Copy the DNS token displayed on the screen, and click **Start Check**.



The status of your domain changes to **Pending**.

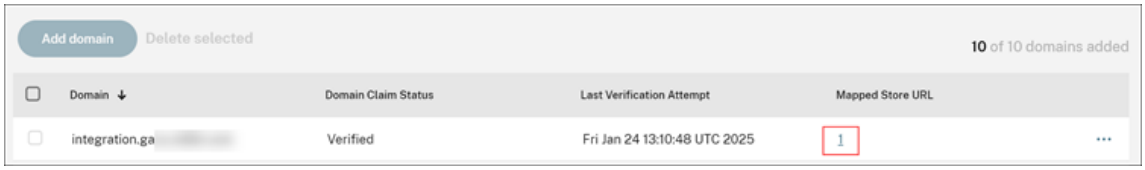
Once the verification is completed, the status of your domain changes from **Pending** to **Verified**.

> **Note:**
>
> You can claim a maximum of 10 domains. If you want to claim more than 10 domains, contact Citrix Support and provide your Customer ID.

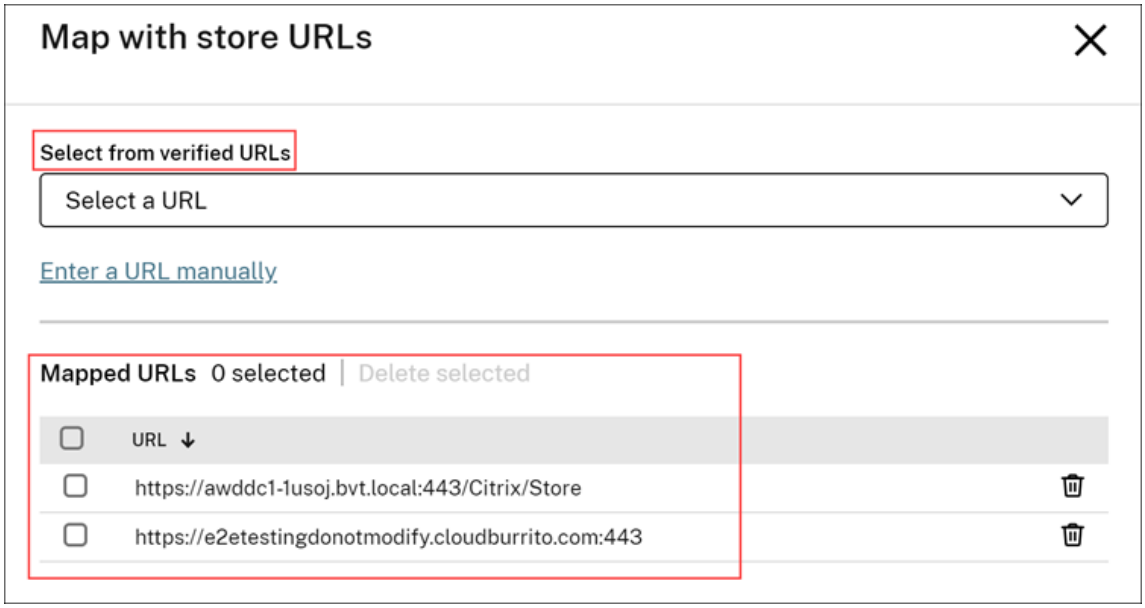
Create a domain to URL mapping

Once the domain is verified, you can map URLs as shown in the following steps:

1. Navigate to **Workspace configuration** > **Email Discovery**.
2. Go to the domain that you have added and click the mapped store URL.



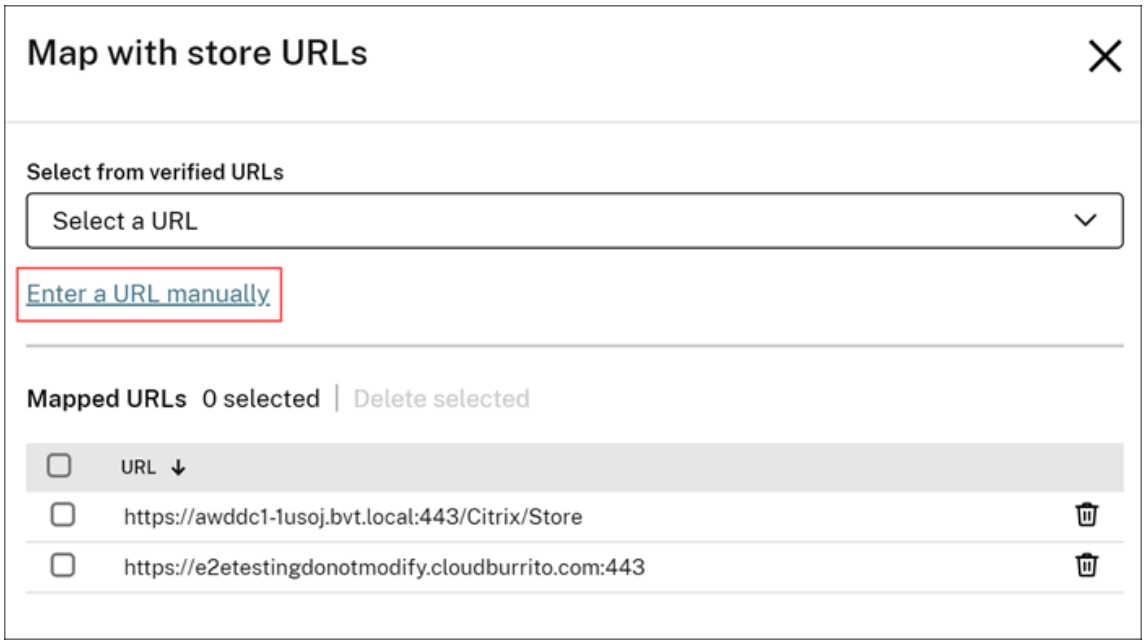
3. Select the claimed URLs from the drop-down menu.



4. Click **Save**.

Alternatively, you can map a URL manually using the **Enter a URL manually** option. For that:

1. Click the **Enter a URL manually** option.



2. Enter the store URL that you want to map to this domain.
3. Click **Add**.

> **Note:**
>
> It is mandatory to include port number 443 in the store URL. For example, https://example.cloud.com:443.

Setup email-based discovery for on-premises stores

To enable email-based discovery for on-premises stores, you need to perform the following steps:

1. Claim a domain
2. Create a domain to URL mapping

Claim a domain

To claim a domain:

1. Go to the AutoDiscovery service.
2. Navigate to **Claims** > **Domains** > **Add Domain**.
3. Enter the domain that you want to claim (for example, ace.example.com).
4. Click **Confirm**.
5. Copy the DNS token that appears on the screen to the clipboard.
6. To create a DNS TXT record, go to the service-provider portal and add the DNS token.
7. To start the verification process:
    a) Navigate to **Claims** > **Domains**.
    b) Go to the domain that you added and click the ellipsis menu.
    c) Select **Verify Domain**.
    d) Click **Start DNS Check**.

Once the verification is completed, the status of your domain changes from *pending* to *verified*.

> **Note:**
>
> You can claim a maximum of 10 domains. If you want to claim more than 10 domains, contact Citrix Support and provide your Customer ID and URL.

Create a domain to URL mapping

To create a domain to URL mapping:

1. Navigate to **Claims** > **Domains**.
2. Go to the domain that you added and click the ellipsis menu.
3. Click **Add Another Server URL**.
4. Enter the store URL that you want to map to this domain and save.

> **Note:**
>
> It is mandatory to include port number 443 in the store URL. For example, `https://storefront.example.com:443`.