# Citrix® StoreFront Cloud

# Contents



# Citrix® StoreFront Cloud Overview

June 22, 2026

Citrix® StoreFront Cloud is a service that provides secure access to your virtual apps, desktops, web and SaaS apps from a web browser or Citrix Workspace app. For an overview of the services available through Citrix® StoreFront Cloud, see Cloud-hosted services through Citrix® StoreFront Cloud.

Citrix® StoreFront Cloud is a cloud service managed by Citrix. If you wish to deploy this functionality in your own environment on-premise then see StoreFront.

Within Citrix® StoreFront Cloud, you can configure one or more stores. End users authenticate to their stores using the selected identity provider. When users launch resources through their store they single sign-on to avoid having to re-enter credentials. For more information on configuring store authentication, visit Configure authentication.

## Get started

See Get started with Citrix® StoreFront Cloud.

## End user access

End-users connect to Citrix® StoreFront Cloud from their devices using either Citrix Workspace app or their web browser. For more information, see User access

## Cloud-hosted services through Citrix® StoreFront Cloud

End users use Citrix® StoreFront Cloud to access the resources provided by cloud-hosted services.

This section describes the main cloud-hosted services that can be enabled for Citrix® StoreFront Cloud, depending on your entitlements.

### Citrix DaaS™

Citrix DaaS is a service that provides app and desktop virtualization, giving IT control of on-prem or cloud-hosted virtual machines, applications, and security while providing anywhere access for any device. End users can use applications and desktops independently of the device's operating system and interface.

If you're an on-premises Virtual Apps and Desktops customer, it is recommended that you first migrate to Citrix DaaS before adopting Citrix® StoreFront Cloud.

#### SaaS and Web apps, secured with the Citrix Secure Private Access™ service

Citrix Secure Private Access provides single sign-on (SSO) to Web and SaaS apps and allows internal web apps to be accessed remotely. The service also allows you to manage access permissions and control policies.

#### Citrix Remote Browser Isolation™ service

Integrate Citrix Remote Browser Isolation service into your stores to isolate web browsing and protect the corporate network from browser-based attacks. When subscribers navigate to the store URL, their published browsers are shown, along with other apps and desktops that are configured in other Citrix Cloud services.

## What's new

June 22, 2026

Product updates are automatically rolled out to all customers when they are available. Depending on the feature, it may be enabled by default for end users or may need to be configured by an administrator, see individual features for more details. Updates are rolled out over a period of a few days so may not be visible immediately.

### July 2026

Citrix® StoreFront Cloud is the new name for Citrix Workspace™. You will see these changes reflected in Citrix Cloud menus, documentation, and the product UI over the coming months.

### June 2026

#### Capability to create multiple custom URLs

You can now add a custom URL for each of your stores. For more information, see Configure a custom domain.

## May 2026

### Resource connectivity options

When Adaptive access is enabled, you can configure different Gateway connectivity depending on whether the user's network location is internal, external or undefined. For more information, see Connectivity options when Adaptive access is enabled.

## March 2026

### Option to prevent ICA downloads

To improve security, you can configure Workspace to prevent users from downloading ICA files. Users must use either Citrix Workspace launcher or Citrix web extensions to launch resources.

For more information, see Prevent ICA downloads.

### Citrix Workspace launcher on iOS and Android

Citrix Workspace launcher is a component of Citrix Workspace app that allows the web browser to detect Citrix Workspace app and launch ICA files in-memory. This improves security by preventing ICA files from being saved to disk. This is now available on iOS and Android.

The first time a user on iOS or Android opens a store website in their browser, or after clearing site data, the website attempts to detect Citrix Workspace app. This requires Citrix Workspace app for iOS or Android 2503 or higher.

If detection completes successfully, subsequently when the user launches apps and desktops, the website invokes Citrix Workspace Launcher rather than downloading ICA files. If the user selects **Skip detection** then the website continues to download an ICA file as it before.

## February 2026

### Enhanced App Protection resource management

Previously when end users accessed their store from a web browser, it only displayed resources requiring App Protection if they installed Citrix Web Extension. You can now choose to always show, or always hide resources requiring App Protection. For more information, see Show or hide resources requiring App Protection.

Version 26.02 removes the dependency on Web extension to launch App Protected resources. Admins can configure App Protected resources to launch on stores that users open in browsers without the

web extension installed. For more configuration details, see App Protection support for hybrid launch through Workspace.

#### Support for Client App Management in hybrid launch scenarios using Citrix Web Extension

Workspace UI (WSUI) release 26.02 provides Client App Management support for hybrid app launches via Citrix Web Extension in cloud deployments.

Hybrid launch refers to signing into Citrix stores from a browser and launching virtual apps and desktops through the locally installed Citrix Workspace app for Windows and Mac.

Users only need to install a supported version of Citrix Workspace app and, where applicable, the Citrix Web Extension.

Minimum supported versions for using this capability:

**Citrix Workspace app:**

**Windows:** Version 2511.1 or later

**macOS:** Version 2511.1 or later

For more details on Client App Management configurations, see Manage settings for hybrid launch.

For more details on Browser Extension, see Citrix web extension.

### December 2025

It is now possible to configure more than 10 Workspace URLs. The default limit remains at 10. If you need more URLs, please contact your Citrix representative.

### November 2025

#### Single Sign-on to VDAs using Entra ID

When authenticating using Entra ID, it is now possible to single sign-on to VDAs without needing FAS. For more information, see Entra ID SSO to VDAs.

### October 2025

#### Citrix Workspace launcher on Linux

Citrix Workspace launcher is a component of Citrix Workspace app that allows the web browser to detect Citrix Workspace app and launch ICA files in-memory. This improves security by preventing ICA files from being saved to disk. This is now enabled on Linux.

The first time a user on Linux opens a store website in their browser, or after clearing site data, the website attempts to detect Citrix Workspace app.

If detection completes successfully, subsequently when the user launches apps and desktops, the website invokes Citrix Workspace Launcher rather than downloading ICA files. If the user selects **Skip detection** then the website continues to download an ICA file as before.

As an alternative, consider installing Citrix web extension, which enables in-memory ICA launch without any additional user interface prompts.

#### Admin consent to stay signed in

Administrators can now provide consent on behalf of end users to Stay signed in. This removes the prompt users otherwise see when they log in to Citrix Workspace app. For more information, see Stay logged in to Citrix Workspace app.

#### Configure Always prompt end users for their credentials per network connectivity type

Administrators can now configure different values of **Always prompt end users for their credentials** depending on the device's network connectivity type. For more information, see Configure sessions per network connectivity type.

### May 2025

#### Inactivity timeouts per connectivity type

Administrators can now configure different inactivity timeouts depending on the device's network connectivity type. For more information, see Configure sessions per network connectivity type.

#### Displays power state of Dedicated desktops

The Workspace User Interface (UI) now provides visibility into the power state of your dedicated desktops. The power state indicates whether a dedicated desktop is Powered On, Powered Off, or in a suspended state (in Hibernation). This enhancement allows users to quickly identify the status of their desktops, enabling them to make informed decisions and manage their resources more effectively.

> **Notes:**
>
> - This feature is enabled by default.
> - This feature is backward compatible with previous versions of Citrix Workspace app.

For more information, see Displays power state of dedicated desktops.

### Configure a custom dialog to be displayed after log in

You can configure a custom dialog that is displayed after users log in. It is displayed on all clients including web, desktop, and mobile devices. You can use it to display information such as company usage policy, or an upcoming maintenance window. Users must accept the dialog before proceeding to their resources.

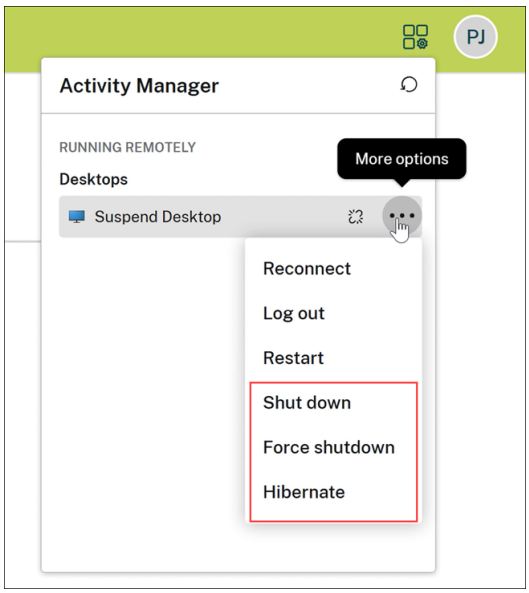
The admin can decide how often the dialog is shown on a per-device basis that is, only once, every day, every 7 days, or every 30 days.

For more information, see Configure a custom dialog to be displayed after log in.

## April 2025

### Enhanced Activity Manager experience and introducing power management control

The Activity Manager feature is now enabled by default, allowing users to disconnect, log out, and restart their virtual sessions. Additionally, administrators can manage the power management controls such as shut down, force shut down, and hibernate virtual sessions using Citrix Cloud.




For more information, see Power management controls.

## March 2025

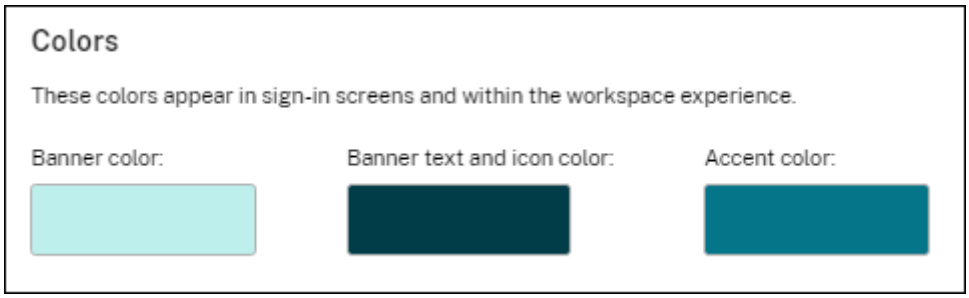
### Color customization applies to Workspace UI elements

This feature introduces enhancements in the following areas:

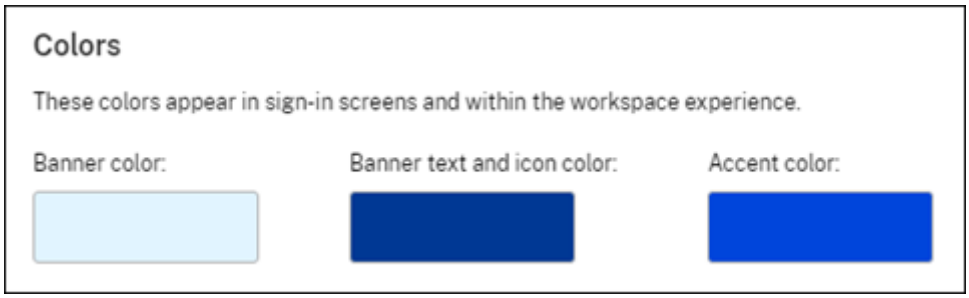
 

- **Full UI Color Customization**: Consistent color scheme now applies to Workspace UI elements.
- **Unified Blue Theme**: A new default blue theme has been implemented to align with common end-user themes across all Citrix apps. Admins can still customize the colors to their preference using Citrix Cloud.

**Old default color:**



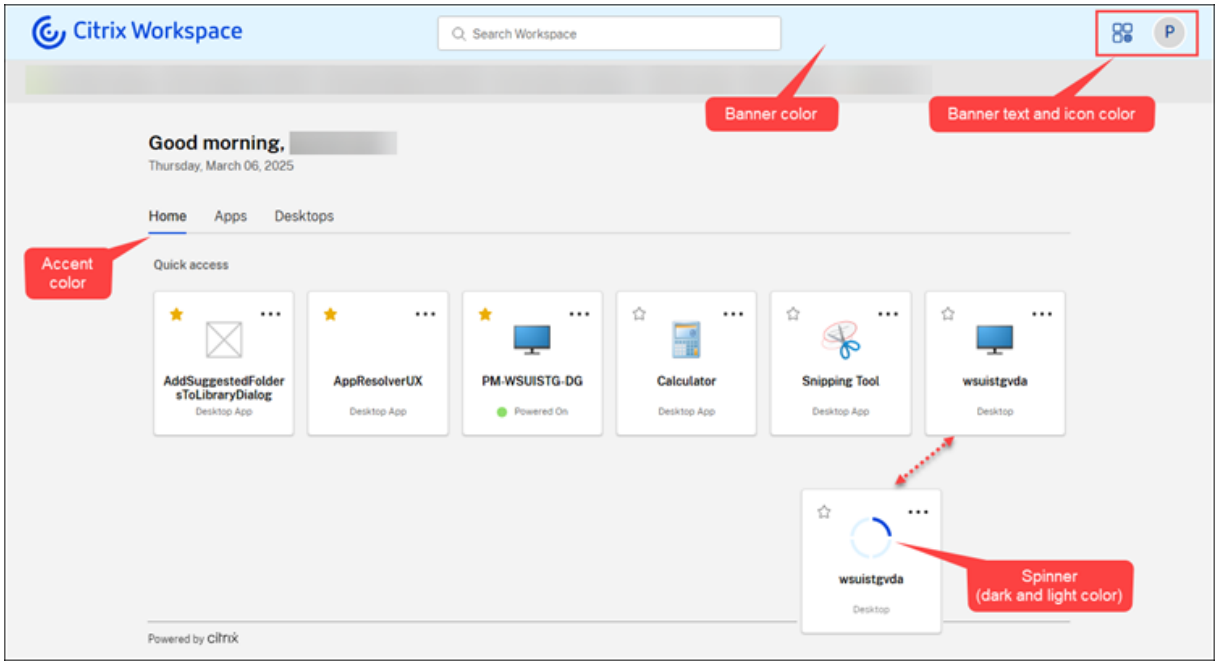

**New default color:**

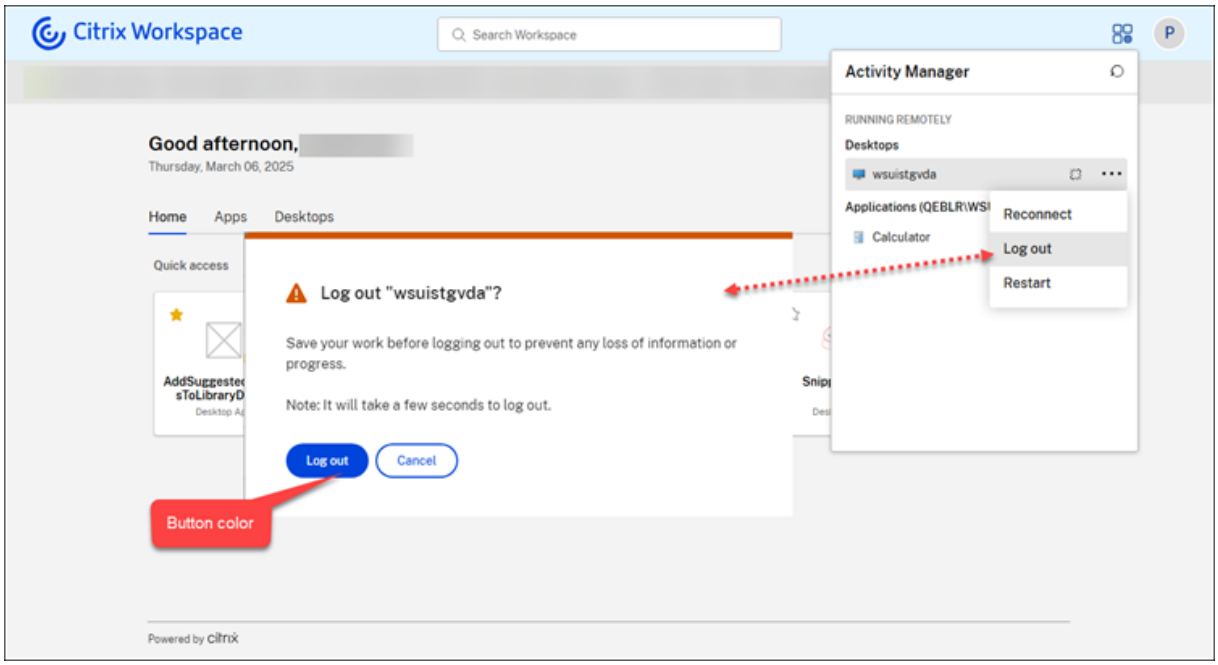



The color change impacts various elements of the UI, including:

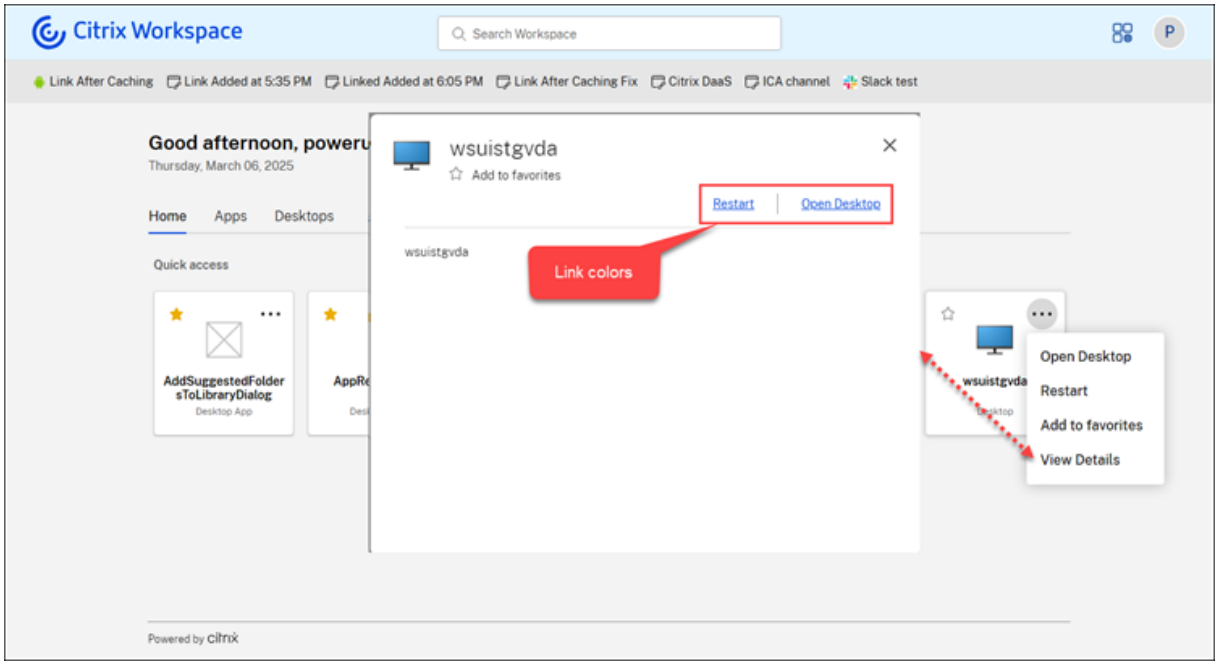
- The banner text and icon color
- The accent, which is a line below certain elements
- The spinner (both the dark and light colors within the spinner)
- Buttons
- Links



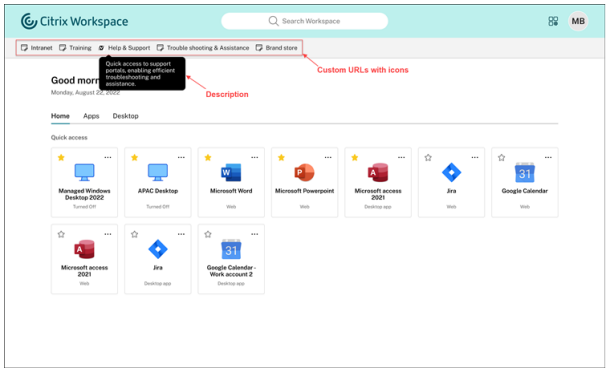

 




For more information, see Customize the appearance of workspaces.

### Pinned links

Pinned links refer to customer-defined hyperlinks that provide quick access to specific websites. This feature functions as a shortcut that helps users to efficiently navigate to websites directly from the Workspace UI. Important links, such as support websites or company portals, can be made available to the users without needing them to search for these links. It makes the navigation effortless and faster.




This feature is supported on both Citrix Workspace web clients and native Citrix Workspace app.

For more information, see Pinned links.

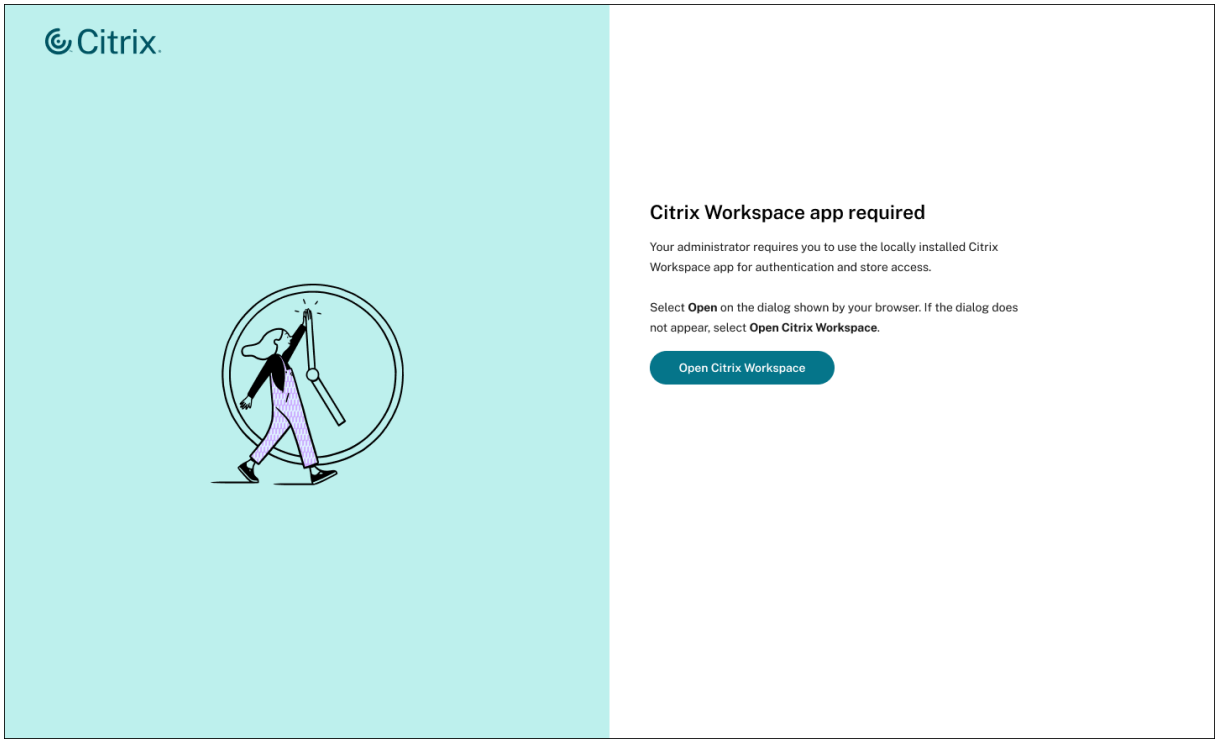
 

## November 2024

### Mandate users to authenticate and open apps and desktops only through the native Citrix Workspace app

Administrators can enforce the use of the native Citrix Workspace app, eliminating the option for users to access the Citrix Workspace web client on browsers. This feature is designed for customers who want to leverage the full benefits of the native app. The native app offers advantages such as built-in App Protection service, no browser version compatibility issues, enhanced security and telemetry for monitoring and troubleshooting.

When the administrators enable this feature, end users see the following webpage when they attempt to access the web client by entering the store URL in a browser.




Once users click **Open Citrix Workspace**, the store is automatically added to the native app for an easier transition from the web client to the native app. This feature is available for Citrix Workspace app for Windows, Mac, Android, and iOS. For more information on compatible native app versions for automatic store addition, see Compatible versions of Citrix Workspace app.

> **Note:**
>
> The feature is applicable to cloud stores for all supported browsers.

For more information, see Customize store access.

### Reconnect and transfer apps and desktops through Activity Manager

Activity Manager introduces reconnect and transfer resource features. The reconnect feature lets end users easily reconnect to disconnected apps and desktops in Citrix Workspace app. The transfer feature allows end users to transfer active sessions from other devices to the current device.

For more information, see Reconnect to disconnected apps and desktops and Transfer your apps and desktops.

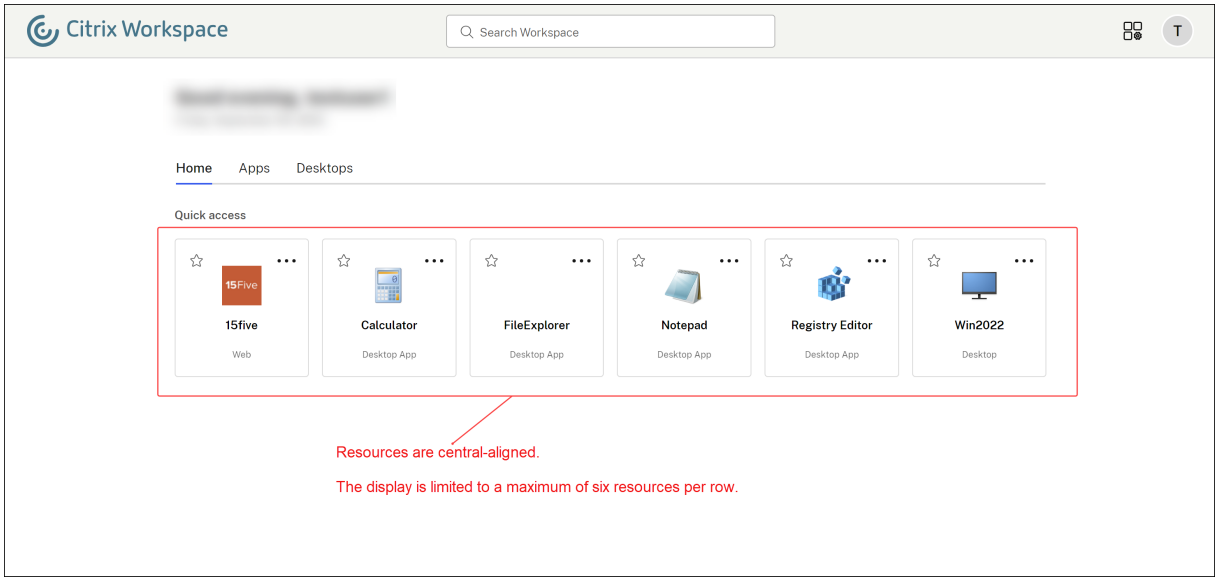
### Custom announcements per Workspace URL

Administrators can now configure different custom announcements depending on the Workspace URL. For more information, see send custom announcement.

## October 2024

### Enhanced UI centralized layout

The Workspace UI has a better resource alignment, unlike the previous layout where resources stretched across the entire width of the screen, the enhanced UI offers a more visually appealing design by centrally aligning the resources and limiting the display to a maximum of six resources per row. This enhanced UI provides a better user experience, leading to improved productivity.

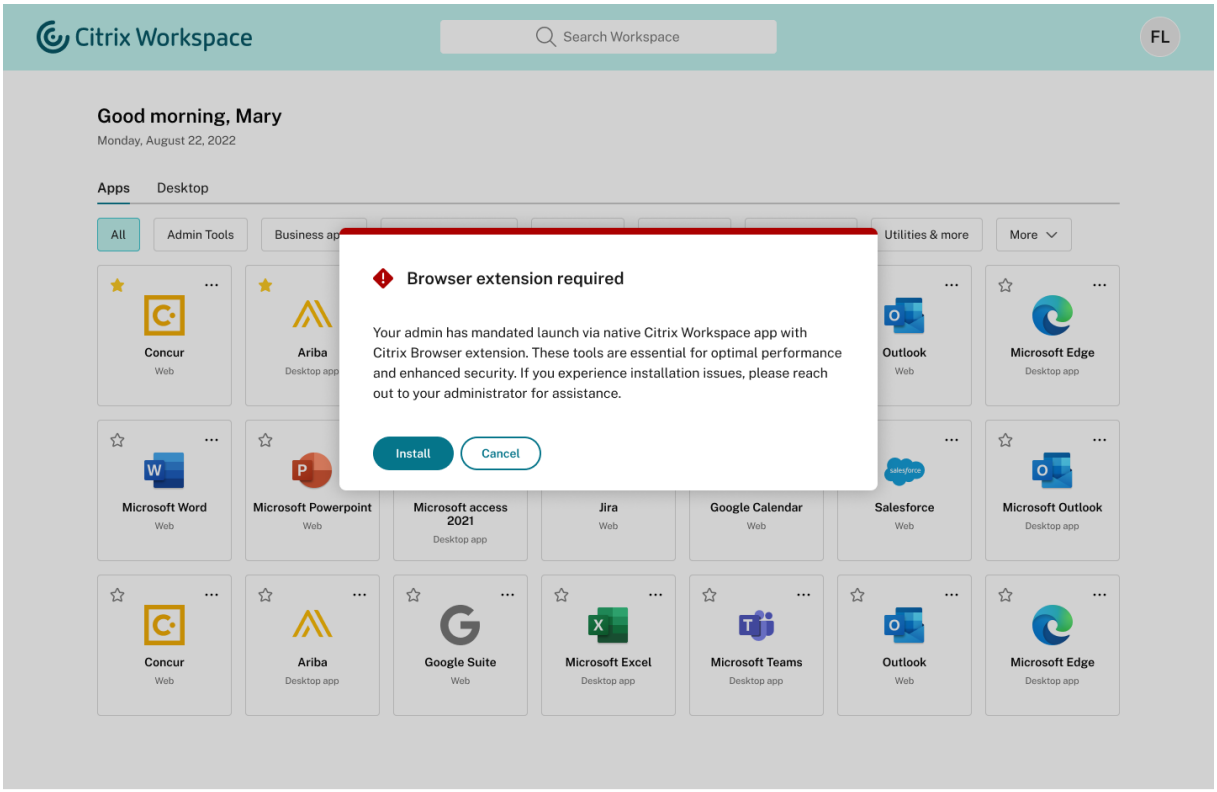


## August 2024

### Manage installation prompt for Citrix Web extension

You can now manage the display of the installation prompt for the Citrix Web extension. Enabling the prompt allows Workspace to detect whether the extension is installed on the user's device when they open Citrix Workspace from a browser. If the extension isn't installed, users are prompted to download and install it. Once users install the extension, it helps to open the apps and desktops in the native Citrix Workspace app automatically without the intervention of Workspace detection screen. As per your preference, you can set the prompt as either mandatory or optional. This prompt feature is compatible with Google Chrome and Microsoft Edge browsers.




When users click the **Install** button, it redirects the users to the respective browser's web extension store, where they can download the Workspace Web extension. The prompt won't appear next time once the user downloads and installs the extension. For more information about managing the prompt, see Launching apps and desktops.

## July 2024

### Configure store names for your store URL

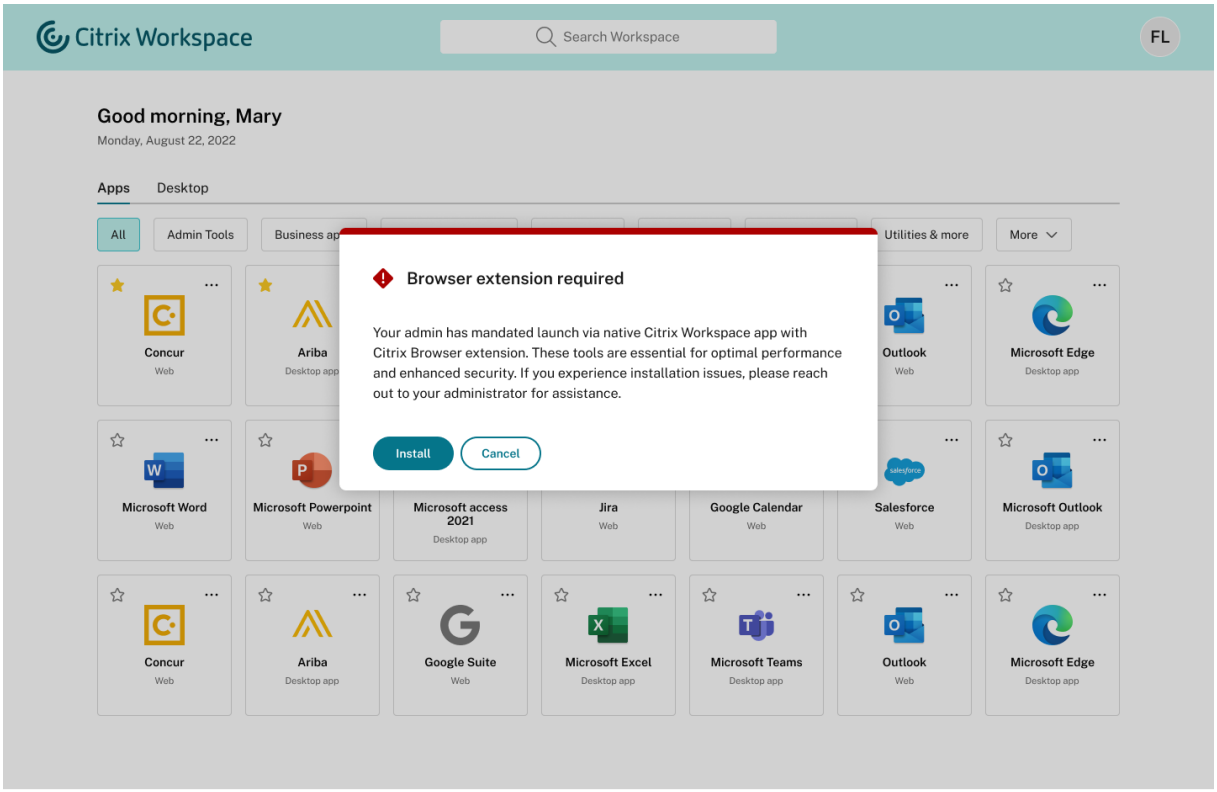
Administrators can now add custom store names while adding stores to Citrix Workspace app. Store names make identifying and distinguishing the stores easier for end users. Previously, in a multiple Workspace URL setup (subdomains of cloud.com), all the stores would be called "Store", with an automatically generated numeric suffix. For example, Store 1, Store 2, Store 3, and so on. This arrangement made it difficult for the administrators and end users to associate the store name with the store URLs.

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

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

**Manage installation prompt for Workspace Web extension** You can now manage the display of the installation prompt for the Workspace Web extension. Enabling the prompt allows Workspace to detect whether the extension is installed on the user's device when they open Citrix Workspace from a browser. If the extension isn't installed, users are prompted to download and install it. Once users install the extension, it helps to open the apps and desktops in the native Citrix Workspace app automatically without the intervention of Workspace detection screen. As per your preference, you can set the prompt as either mandatory or optional. This prompt feature is compatible with Google Chrome and Microsoft Edge browsers.




When users click the **Install** button, it redirects the users to the respective browser's web extension store, where they can download the Workspace Web extension. The prompt won't appear next time once the user downloads and installs the extension. For more information about managing the prompt, see Launching apps and desktops.

### Deprecation of old Workspace UI

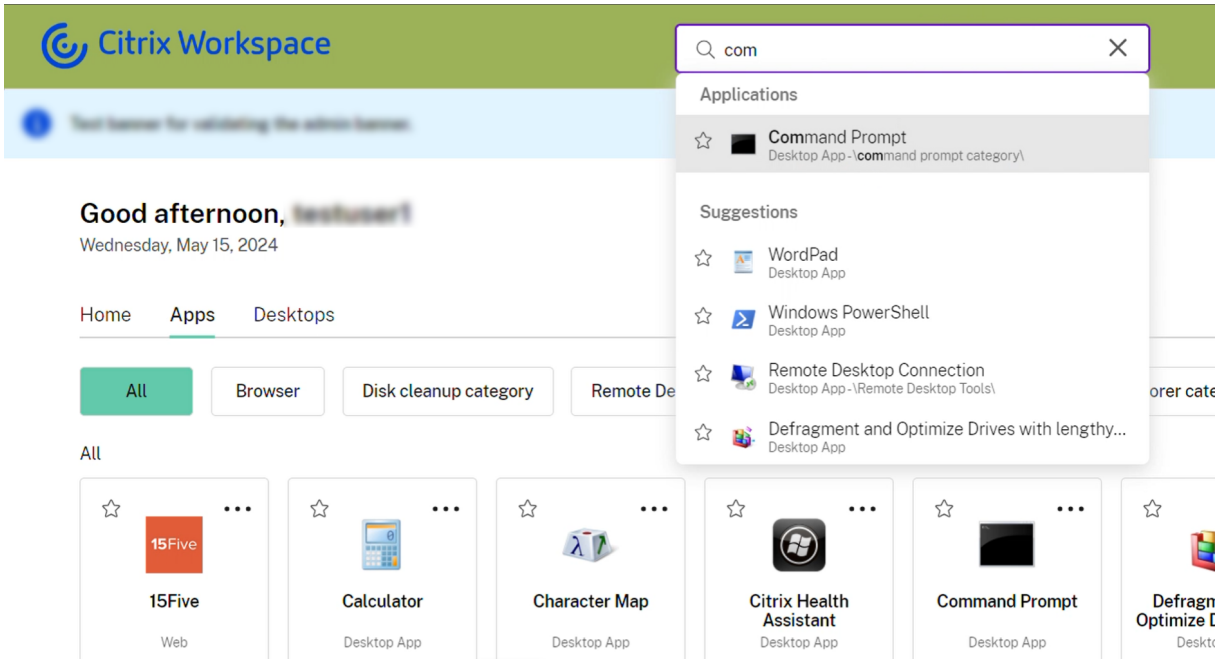
The old Workspace UI experience is now deprecated. Administrators no longer have the option to enable the old UI for end users. The new Workspace UI offers a better user experience and increases productivity, and it is enabled by default.

## May 2024

### Enhanced search experience

The Citrix Workspace app introduces an enhanced search engine feature, allowing end users to view the app path alongside search results. This functionality assists end users in quickly identifying an app's location. Long app paths are truncated to maintain a clean and uncluttered search results list. You can see the complete path when hovering the mouse pointer over the path's breadcrumb. Additionally, the category name will be highlighted in bold for easy recognition if it matches the search input.




**Performance improvement**

Citrix Workspace UI now loads faster than before after the enhancements in the following areas:

**1. Parallelizing user authentication and Workspace UI loading** Citrix Workspace UI loads quickly while the user authentication check runs in the background. Unlike previous Citrix Workspace UI, the new version stores cache data locally of previous sessions and reuses it for quicker app opening. Consequently, the app no longer requires users to wait for authentication checks to complete.

Previously, users could access the app only after the authentication checks were complete. This delay of around 1-2 seconds has now been rectified, allowing returning users to enter the store url and start accessing the Workspace UI while the user authentication check runs in the background. If the user session is found to be not logged in during the background check, the app prompts the user for authentication to continue the session. Additionally, the app continues to refresh app data in the background so that this data can be used in subsequent sessions.

**2. Caching Workspace UI** The Workspace UI now loads from cache, resulting in quicker opening of the app than before. Additionally, Workspace UI refreshes itself in the background to fetch the latest version of UI whenever the user minimizes the Workspace app, switches to another browser tab from Workspace web app tab or reloads the app.

> **Note:**
>
> The performance improvement is applicable when using both a web browser and Citrix Workspace Web app.

#### Hibernate and Resume virtual desktop sessions

Users can now hibernate their virtual desktop sessions on Citrix Workspace app when not in use and resume them from where they left off. The hibernate action preserves the entire state of the desktop session, including the running apps. The feature allows the users to seamlessly resume their sessions upon signing back again. When resumed, the desktop session launches faster compared to stopped or deallocated virtual desktops.

Citrix Activity Manager's Hibernate and Resume feature represents a significant advancement in VDI management, offering organizations a powerful tool to optimize resource utilization and enhance user experience. This feature efficiently manages resources, improves user experience, and reduces energy consumption during hibernation, resulting in significant cost savings.

For more information on configuring this feature on user devices and performing hibernation and resume operations, see Hibernate and Resume virtual desktop sessions.

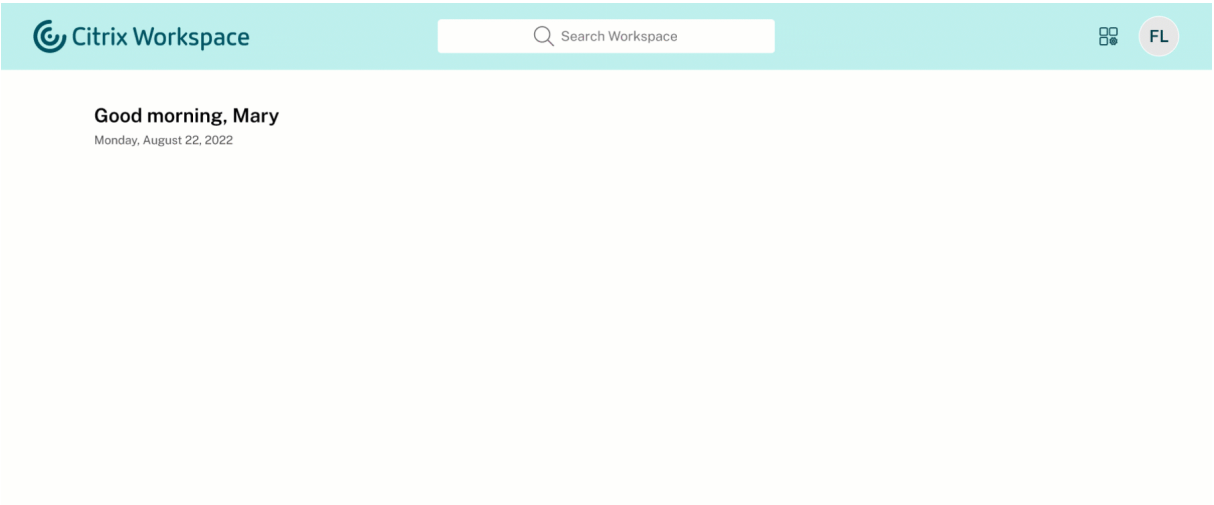
### March 2024

#### Activity Manager has manual refresh option

With this release, end users can now manually refresh the list of items within the **Activity Manager** for the cloud store, accessible on both desktops and mobile devices. They are no longer required to restart the **Activity Manager** to see the updated list. Two options are available to refresh the list: a refresh button and a refresh icon. End users can use the **Refresh** button when the **Activity Manager** screen is empty, and they can use the refresh icon  to update the existing list. This new feature enhances the end user experience by allowing them to manage the sessions within the **Activity Manager** more efficiently and conveniently.

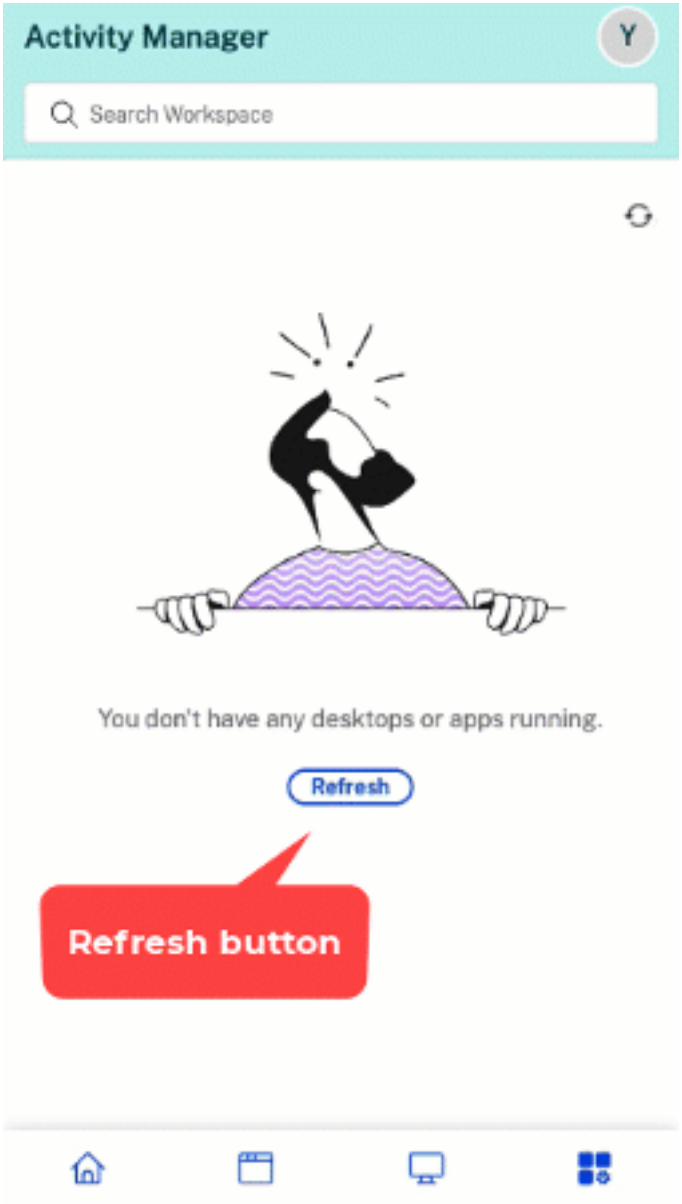
**Activity Manager on desktop version:**




**Activity Manager on mobile version:**

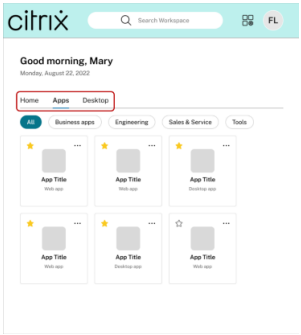
 




**Disable Simple View of Workspace UI**

Currently, when users launch Citrix Workspace app with fewer than 20 resources, they see the screen with Simple View where users don't see navigation tabs, like Home, Apps, and Desktops. All the apps and desktops are consolidated on one page and administrators don't have the control to disable this view. With this release, you can disable the Simple View and customize the new Workspace UI as per your preference.




Even if the number of resources are less than 20, you can still use the navigation tabs if you prefer a consistent view for your users. For more information on how to manage the Simple View, see Simple view.

## Feb 2024

### Create multiple Workspace URLs - General Availability (GA)

The multiple Workspace URL feature is now generally available for all users. You can now create multiple Workspace URLs (subdomains of cloud.com) and use these URLs as policy inputs. For example, you can configure different URLs for different subsidiaries or divisions within your organization. Each of these URLs can have different branding, authentication methods, or desktops and apps.

> **Note:**
>
> You can create a maximum of 10 URLs for your Workspace.

Each store is accessible by a unique URL can differ in the following aspects:

- Branding of the UI (post login)
- Apps and desktops
- Authentication configuration (such as different identity providers)

For more information, see Configure multiple Workspace URLs.

## Support for Finnish language

Citrix Workspace UI is now available in the Finnish language.

## Dec 2023

### Create multiple Workspace URLs (Technical Preview)

You can now create multiple Workspace URLs (subdomains of cloud.com) and use these URLs as policy inputs. For example, you can configure different URLs for different subsidiaries or divisions within your organization. Each of these URLs can have different branding, authentication methods, or desktops and apps.

> **Note:**
>
> You can create a maximum of 10 URLs for your Workspace.

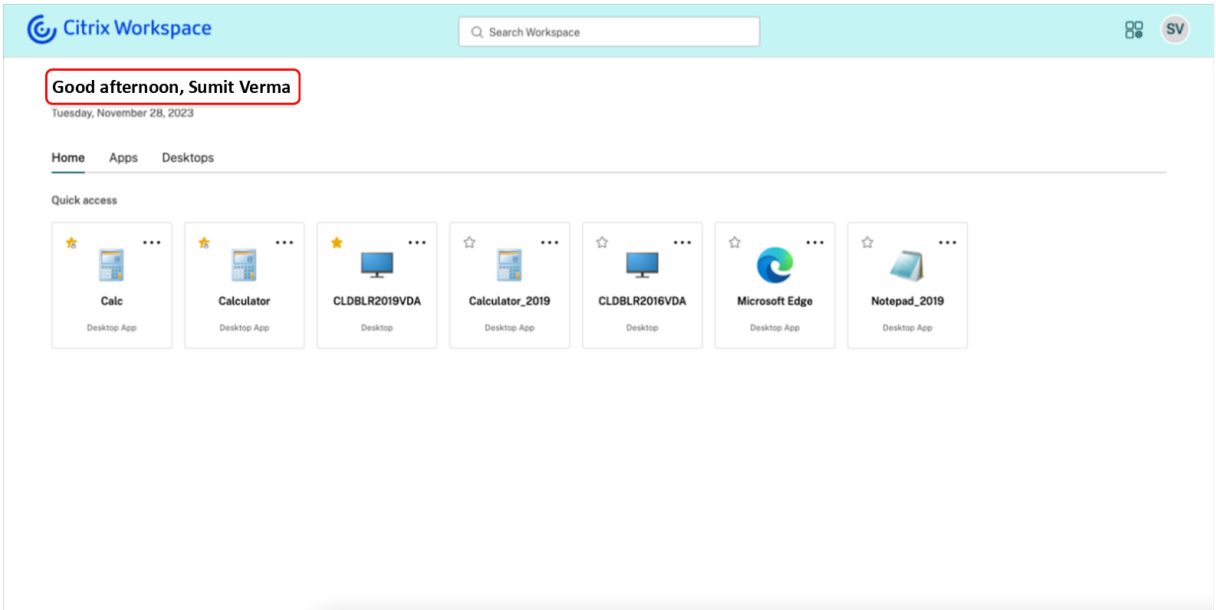
Each store is accessible by a unique URL can differ in the following aspects:

- Branding of the UI (post login)
- Apps and desktops
- Authentication configuration (such as different identity providers)

For more information, see Configure Workspace URLs.

### View user's display name and profile picture on Workspace UI

With this release, users can now view their display name and profile picture on the Workspace UI. The user's display name is shown along with the greetings. The profile picture, initials, or a generic image appears on the user menu at the upper-right corner. Admins must note that Workspace UI displays this information only if the Active Directory fetches valid data.




For more information, see Manage user's display name and profile picture

## Nov 2023

### Configure a custom domain - General Availability

The Custom Domain feature is now generally available. You can configure a custom domain for your workspace, which allows you to use a domain of your choice to access your Citrix Workspace store. You can then use this domain in place of your assigned cloud.com domain for access from both a web browser and Citrix Workspace applications. For more information, see Configure a custom domain.

## Removal from Google indexing

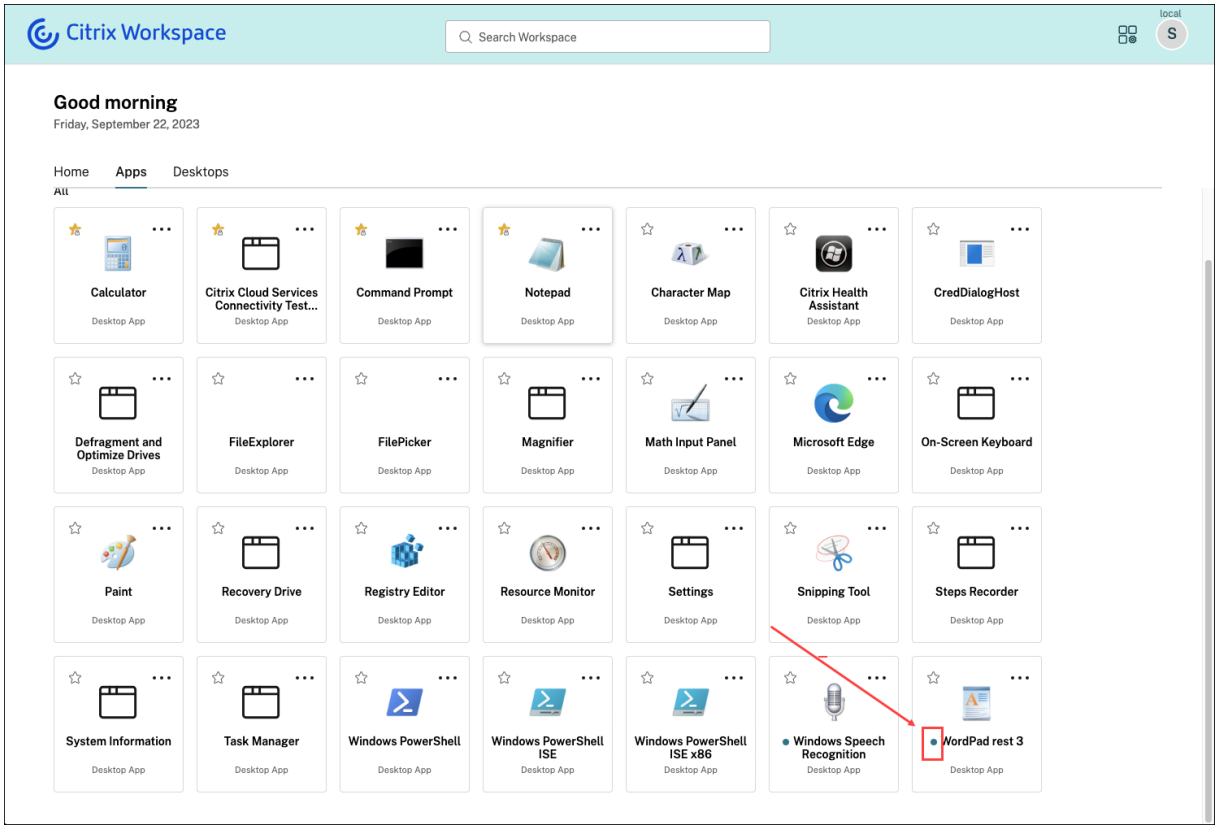
Google Search indexing has been removed from Citrix Workspace to prevent Workspace URLs from appearing in Google's search results. However, if your URLs have already been indexed by Google, you must take steps to remove them. For more information, see Remove a page hosted on your site from Google.

## October 2023

### Streamlined discovery of new apps

End users can now easily spot newly added apps, making it easier to explore and utilize the latest apps. When an admin delivers a new app to an end user, it is highlighted on the end user's workspace and a green dot is displayed on the app tile for the first time.




## September 2023

The new Workspace user interface is now generally available. It introduces new UI capabilities with a modern look and feel for a cleaner view. The UI enhancements are applicable for web, desktops, and mobile. Admins can enable it for their end users from Workspace **Configuration** > **Customize** > **Features**. For more information, see User experience.

> **Note:**
>
> By default, the new UI toggle will be in a disabled state for the next 6 months unless enabled by admins. After 6 months, the new UI will be enabled for all users by default and the current UI experience will be deprecated. Admins need to transition their users to the new UI within the next 6 months.

### Activity Manager

The Activity Manager feature is now generally available on the new UI for cloud. Activity Manager is a simple yet powerful feature that empowers users to effectively manage their resources.It enhances productivity by facilitating quick actions on active and disconnected apps and desktops

from any device. Admins can enable this feature for their end users from Workspace **Configuration**>**Customize**>**Features**>**Activity Manager**.

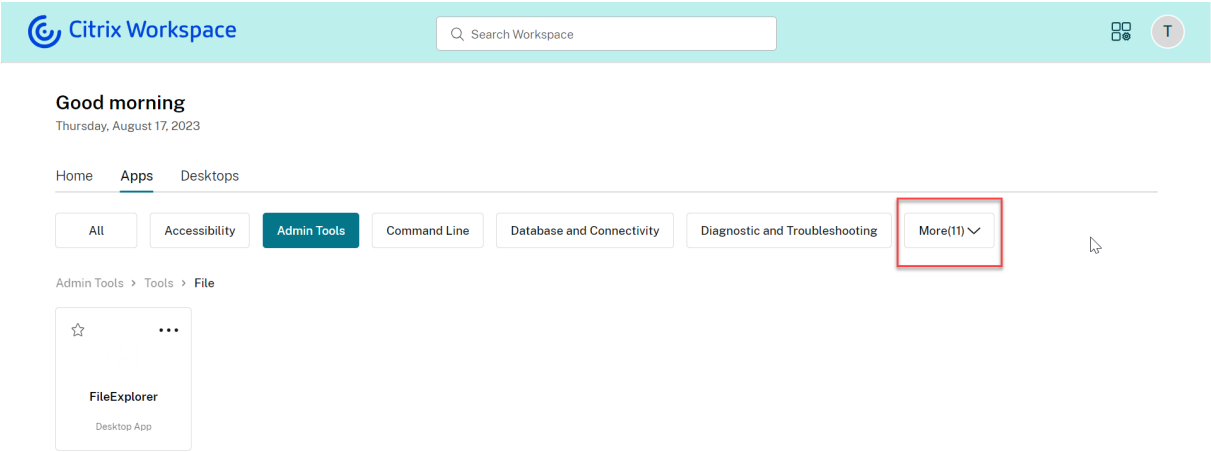
Once enabled, apps and desktops that are either active or in a disconnected state are displayed on the Activity Manager panel. Apps are grouped under their respective sessions. End users can click the ellipses (...) icon to take quick actions:

- **Disconnect**: Disconnects the remote session but the apps and desktops are active in the background.
- **Log out**: Logs out from the current session. All the apps in the sessions are closed, and any unsaved files are lost.
- **Shut Down**: Closes your disconnected desktops.
- **Force Quit**: Forcefully powers off your desktop in case of a technical issue.
- **Restart**: Shuts down your desktop and start it again.

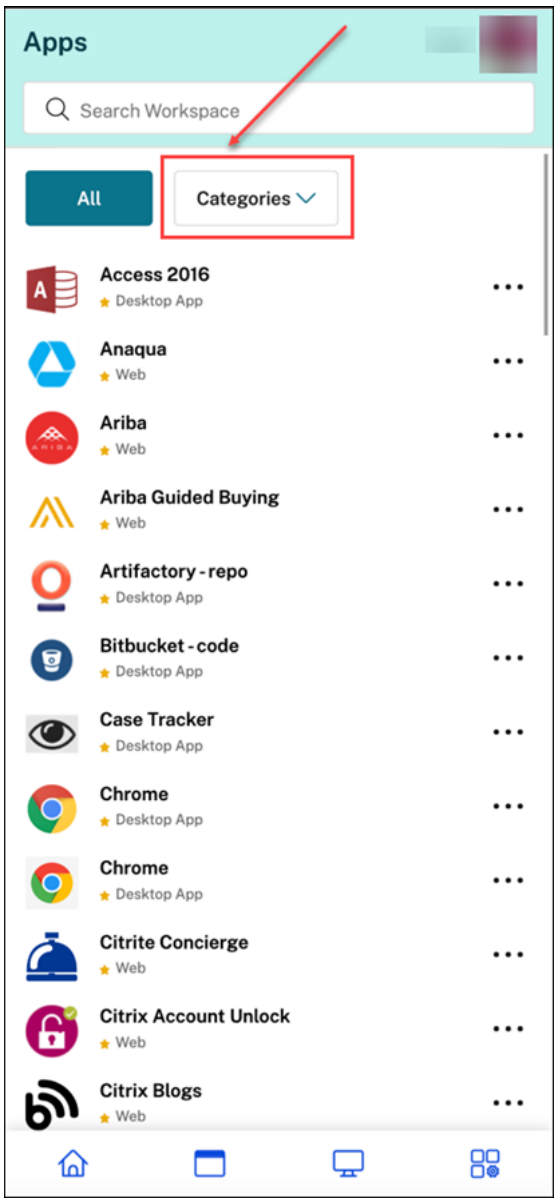
For more information, see Activity Manager.

### App categorization

End users can view their applications organized into categories and sub-categories on the Workspace user interface. If the categorization involves more than two levels, end users will see their applications arranged within a folder structure. The navigation breadcrumbs are visible to the users.
When the number of primary categories created by the admins exceeds the available space on the user's screen, the user interface adjusts based on the screen size, and dynamically moves categories under the **More** dropdown.

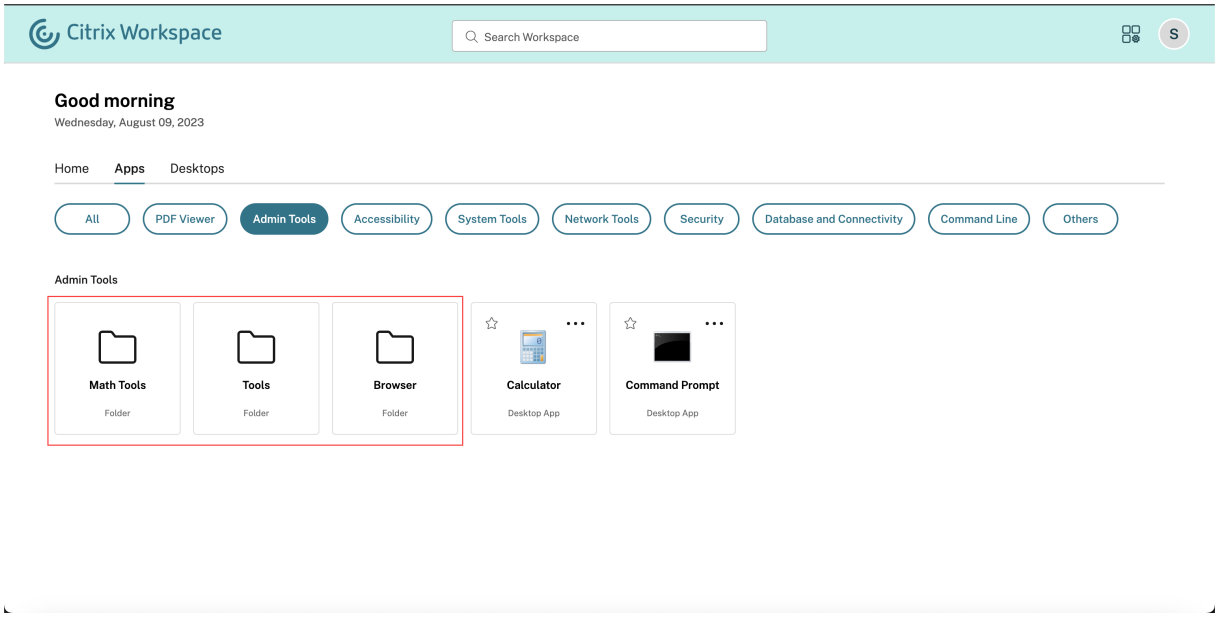


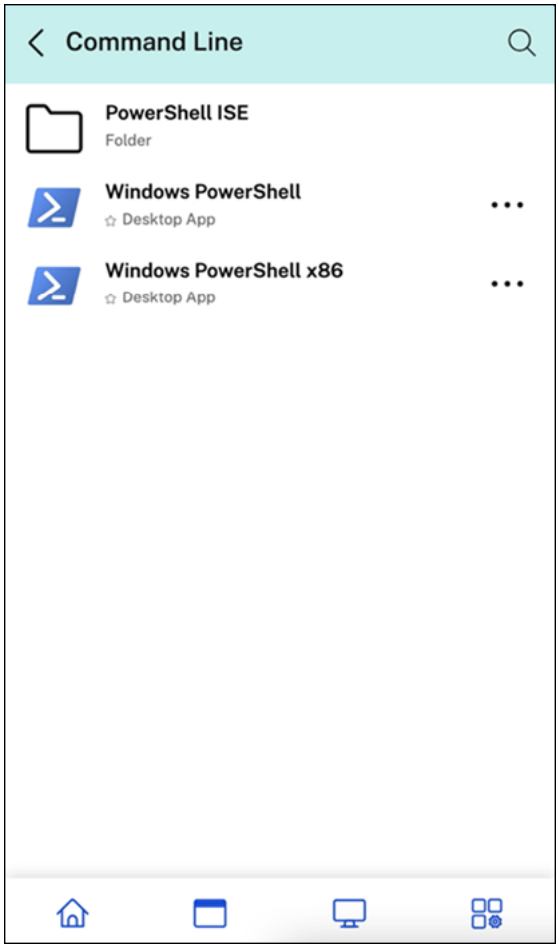

 




From the second level of categorization, end users will see a folder structure. The organized multi-level structure makes for a clutter-free, optimized experience that helps enhance the overall user satisfaction. For more information on creating folders and sub-folders, see Create delivery groups.



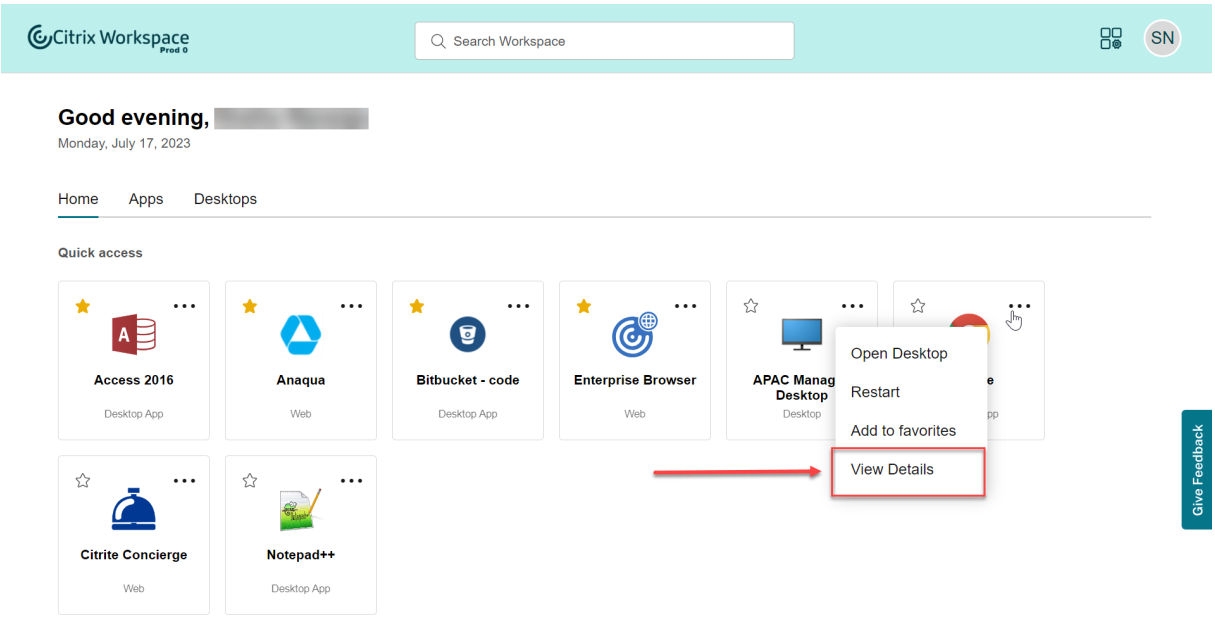

For more information, see Add folder path

### View description of apps and desktops

End users can now view the description provided by admins for apps and desktops. These descriptions aid in comprehending the intended functionality of an app or desktop. They are especially useful in case multiple apps exist with the same name but differ in their configuration, location, environment, etc.

To view the description of an app or desktop, click ellipses on the respective tile and then click **View Details**.




### Enhanced first-time user experience

When you launch the downloaded or Citrix from a browser for the first time, you're prompted with a screen that lists the relevant apps. These apps are decided by the admin, and you can add these apps as favorites with a single click.

### Enhanced search experience

The enhanced **Search** feature gives you faster results from the search engines. The **Search** option allows you to do a quick and intuitive search from within the Workspace app.

### Deprecation announcement for Internet Explorer

Support for Internet Explorer is deprecated and will be removed in the last week of 2023. Until then, Internet Explorer will display the legacy user interface without any new features, bug fixes, or security patches.

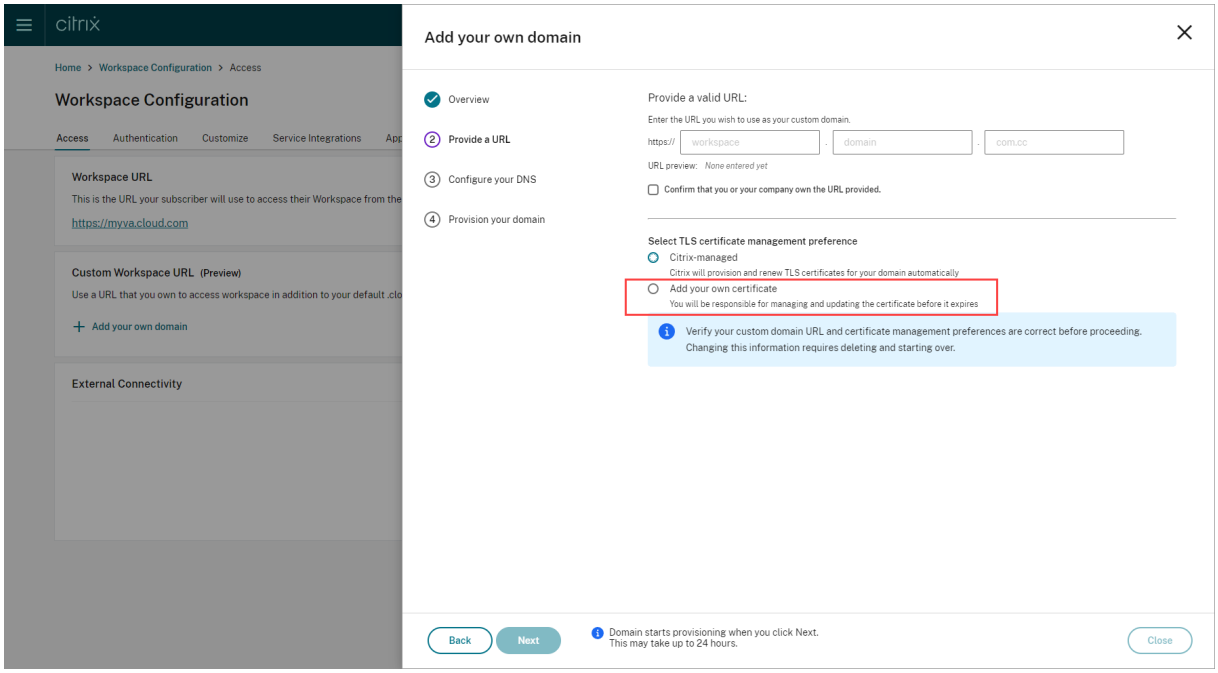
## August 2023

### Add your own TLS certificate for custom domain (Preview)

You can now upload your own TLS certificate for authentication while configuring a custom Workspace URL. Before uploading a certificate, ensure that the certificate fulfills the following conditions.

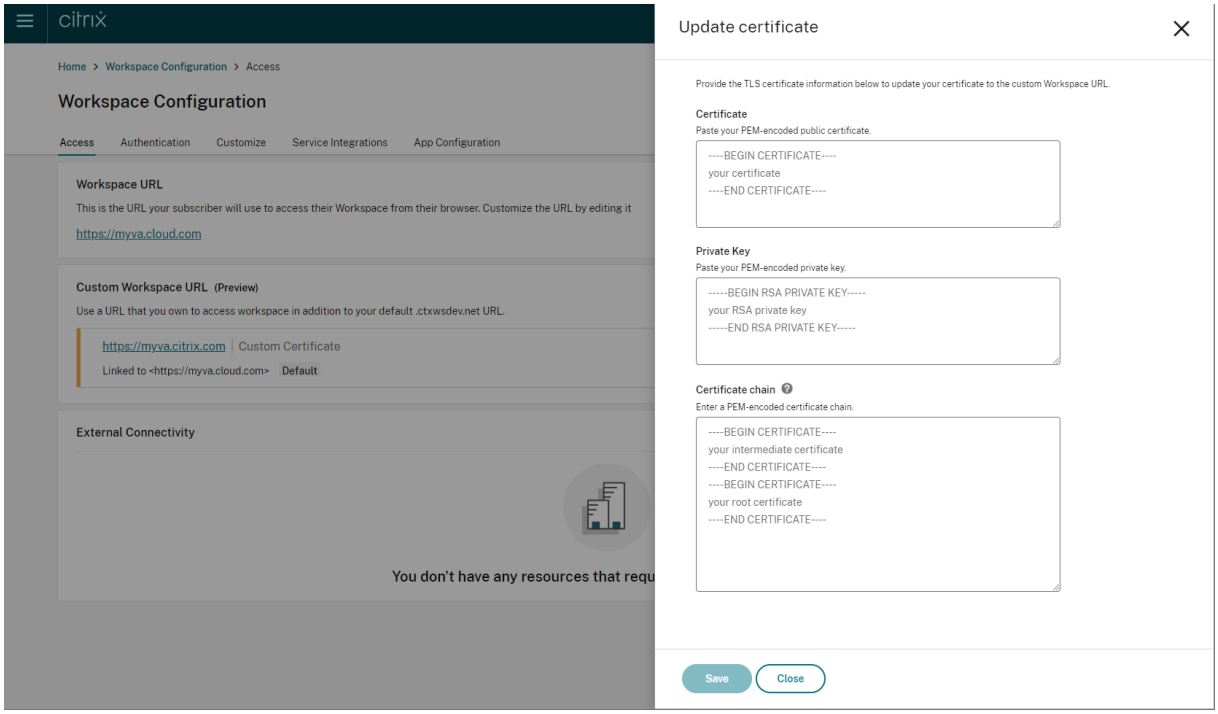
- It should be PEM encoded.
- It should remain valid for at least next 30 days.
- It should be used exclusively for custom Workspace URL, wildcard certificates are not acceptable.
- The common name of the certificate should match the custom domain.
- SANs on the certificate should be for the custom domain, any additional SANs are not allowed.
- The duration for which the certificate is valid should not exceed 10 years.

To add your certificate, navigate to the **Provide a URL** page, and select the Add your own certificate option under **Select TLS certificate management preference**.




You can then add your certificate on the **Add your own certificate** page.




For more information, see Adding a custom domain.

### May 2023

**Configure a custom domain (Preview).** You can configure a custom domain for your workspace, which allows you to use a domain of your choice to access your Citrix Workspace store. You can then use this domain in place of your assigned cloud.com domain for access from both a web browser and Citrix Workspace applications. For more information, see Configure a custom domain (Preview).

### March 2023

**Additional inactivity timeout settings:**. You can now enable extra inactivity timeout settings for both desktop and mobile users of Workspace app. For more information, see Customize security and privacy policies.

### December 2022

**Additional send custom announcement configuration option:**. You can now set the page placement when configuring **Send custom announcement** to either top or bottom. For more information, see Customize security and privacy policies.

**Support for Traditional Chinese language.** Citrix Workspace is now available in the Traditional Chinese language.

### October 2022

**Support for Korean language.** Citrix Workspace is now available in the Korean language.

**Support to customize Citrix Workspace app settings.** Administrators can now configure the settings for Citrix Workspace app for iOS, Android, HTML5, Mac, and Windows platforms using the Global App Configuration service.

### August 2022

**Improvements to Workspace launch experience.** When a user launches their workspace over web or browser, a notification is triggered showing the launch status. If the user attempts to close the browser when a launch is in progress, the user is prompted for confirmation and informed that a session launch is in progress. For more information, see Get started with Citrix Workspace.

### June 2022

**Support for service continuity with Safari.** Citrix Workspace Web extensions make service continuity available to users who access their apps and desktops through a browser. For more information, see Service continuity in browser.

### May 2022

***New configuration option for federated identity provider:** Enable or disable your federated identity provider to allow your end users to be prompted to authenticate when logging in to Workspace. For more information, see Customize workspace interactions.

**Reauthentication period for Workspace app general availability:** Reauthentication periods allow end users to stay signed in to Workspace without being prompted to sign in every time they access their workspace. When signing in through Workspace app, end users consent to stay signed in. End users remain signed in during the reauthentication period as long as they're using their apps and desktops. For more information about this feature, see Stay logged in to Workspace app.

**Support for service continuity on iOS:** Service continuity is now supported for Citrix Workspace app for iOS in general availability. For more information, see Service continuity.

**New error codes for service continuity:** New error codes are now available to aid in troubleshooting failed service continuity connections. For more information, see Service continuity.

### March 2022

**Support for service continuity on Android and iOS:** Service continuity is now supported for Citrix Workspace app for Android in general availability and Citrix Workspace app for iOS in technical preview. For more information, see Service continuity.

### February 2022

**Support for service continuity with Citrix Workspace app for Android (general availability) and Citrix Workspace app for iOS (technical preview):** Service continuity allows users to connect to their virtual apps and desktops even during outages. It is now supported for Citrix Workspace app for Android in general availability and Citrix Workspace app for iOS in technical preview. For more information, see Service continuity.

**Send custom announcement and custom sign-in policy:** Two new features are now available for all customers. These features allow Workspace administrators to display their own post-login persistent banner and pre-login custom message or license agreement in Citrix Workspace app. For more information, see Custom announcements and Log in dialog

### December 2021

**Remove the default, split sign-in screen for employee and client users of Citrix Content Collaboration:** Citrix Workspace now allows you to enable a single sign-in flow for both client and employee users.

**Support for service continuity in browser with Citrix Workspace app for Mac:** Citrix Workspace Web extensions make service continuity available to users who access their apps and desktops through a browser. This feature now is supported on devices running Citrix Workspace app for Mac. For more information, see Service continuity.

### November 2021

**Policy-driven theming:** You can create and prioritize Workspace themes, and add each theme to different user groups in **StoreFront Cloud**. For more information, see Customize the appearance of workspaces.

### October 2021

**Electronic signature language support:** Electronic signature now offers support for Italian and Brazilian Portuguese in addition to the following languages: German, French, Spanish, Japanese, Dutch, and Simplified Chinese. For more information, see RightSignature multi-language support.

**FAS support for multiple resource locations general availability:** Citrix Workspace now supports providing single sign-on to virtual apps and desktops across multiple resource locations. Also, FAS servers in one resource location can be designated as primary or secondary to provide failover for FAS servers in other resource locations. For more information, see Enable single sign-on for workspaces with Citrix Federated Authentication Service.

### September 2021

**Citrix Workspace app for HTML5 introduced to Citrix Workspace:** Citrix Workspace app for HTML5 delivers the Citrix Workspace experience in browsers without any installation on the device. For more information about Citrix Workspace app for HTML5, including new features, visit the Citrix Workspace app for HTML5 product documentation.

**Support for service continuity in browser general availability:** Citrix Workspace Web extensions make service continuity available to users who access their apps and desktops through a browser. This feature is for Google Chrome and Microsoft Edge on Windows devices. For more information, see Service continuity in browser.

### July 2021

**Custom end user license agreement policy:** You can present end users with a custom usage agreement policy to read and accept before they sign into their Workspace. For more information about this feature, see Configure a sign-in policy.

**Reauthentication period for Workspace app preview:** Reauthentication periods allow end users to stay signed in to Workspace without being prompted to sign in every time they access their workspace. When signing in through Workspace app, end users consent to stay signed in. End users remain signed in during the reauthentication period as long as they're using their apps and desktops. For more information about this preview feature, see Set a reauthentication period for Citrix Workspace app.

**Network location configuration through Citrix Cloud:** You can now configure network locations through the Citrix Cloud management console in addition to using the Citrix-provided PowerShell script. For more information about this feature, see Optimize connectivity to workspaces with Direct Workload Connection.

### June 2021

**FAS support for multiple resource locations preview:** Citrix Workspace now supports providing single sign-on to virtual apps and desktops across multiple resource locations. FAS servers in one resource location can be designated as primary or secondary to provide failover for FAS servers in

other resource locations. For more information about this preview feature, see Enable single sign-on for workspaces with Citrix Federated Authentication Service.

**Support for service continuity in browser technical preview:** Citrix Workspace Web extensions make service continuity available to users who access their apps and desktops through a browser. This technical preview is for Google Chrome and Microsoft Edge on Windows devices. For more information, see Service continuity in browser.

**Service continuity general availability:** Service continuity allows users to connect to their virtual apps and desktops even during outages in Citrix Cloud components or in public and private clouds. For more information, see Service continuity.

**Citrix RightSignature app available:** Take advantage of Citrix app, an electronic signature solution that comes with Workspace Premium and Premium Plus to request e-signatures on documents on any device through Citrix Workspace. For more information, see Configure Citrix RightSignature app.

### May 2021

**Custom themes technical preview:** Customizing the appearance of Workspace for end users now supports custom themes that you can assign to different user groups. Create, customize, and prioritize themes so end users in those user groups see their appropriate workspace theme when they sign in. For more information, see Customize the appearance of workspaces.

**Electronic signature language support:** Electronic signature capability now offers support for the following languages: German, French, Spanish, Japanese, Dutch, and Simplified Chinese. For more information, see RightSignature multi-language support.

### February 2021

**Account password changes:** End users can change their domain password from within Citrix Workspace. Administrators can also provide password guidance to end users for creating valid complex passwords in accordance with their organization's password policy. For more information, see Allow end users to change their account password.

### December 2020

**Service continuity technical preview:** Service continuity allows users to connect to their Citrix DaaS even during outages in Citrix Cloud components or in public and private clouds. For more information, see Service continuity.

### May 2020

**Get Started with Citrix Workspace guide:** Citrix Workspace now includes a step-by-step walkthrough to help you deliver workspaces quickly to your end-users. The walkthrough guides you through the Citrix Cloud console so you can configure an identity provider, add administrators, and enable workspace authentication and services. For an overview of the tasks and quick access to the instructions you need, see Get Started with Citrix Workspace.

### December 2019

**Network Location Service:** You can now ensure that users who launch apps and desktops in Workspace from within the corporate network are routed directly to their VDAs. This bypasses the gateway and results in faster DaaS sessions. For more information about this service and setup instructions, see Optimize connectivity to workspaces with the Network Location Service.

**Improvements for Recent and Favorite apps:** Recents and Favorites are loaded first in Workspace, so users can launch their commonly used apps and desktops right away.

## Get started with Citrix® StoreFront Cloud

June 22, 2026

This article outlines the main steps involved in setting up Citrix® StoreFront Cloud and related components, from beginning to end. For a summary of the steps involved, see Workflow overview.

If you are setting up Citrix® StoreFront Cloud, there are the following broad steps:

1. Prepare for Citrix® StoreFront Cloud in Citrix Cloud™.
2. Configure end-user access and authentication.
3. Customize stores with your enterprise-specific preferences, such as logos and security policies.
4. Configure store resiliency and optimization.
5. Roll out Citrix® StoreFront Cloud to end-users.

### Migration from StoreFront

If you are an existing customer using NetScaler and StoreFront then consider the following:

- It is recommended that you first migrate from on-prem CVAD deployments to DaaS before you migrate from on-prem StoreFront to Citrix® StoreFront Cloud. For more information, see Migrating from on-premises to cloud and the Tech Zone deployment guide. You can transition to

Citrix® StoreFront Cloud with your existing on-premises Virtual Apps and Desktops deployment. This process is called site aggregation. This has performance and resilience limitations so is only recommended for simple deployments.

- You can configure your existing NetScaler gateway as an IdP for authenticating end-users. However in many cases it can be replaced by one of the other authentication methods available in Citrix Cloud. For mroe information see Identity and access management.
- You can continue to use your NetScaler gateway as an HDX proxy for remote access to DaaS resources. However it is recommended that you instead migrate to Citrix Gateway Serice. For more information, see External connectivity.

### Step 1: Prepare for Citrix® StoreFront Cloud in Citrix Cloud

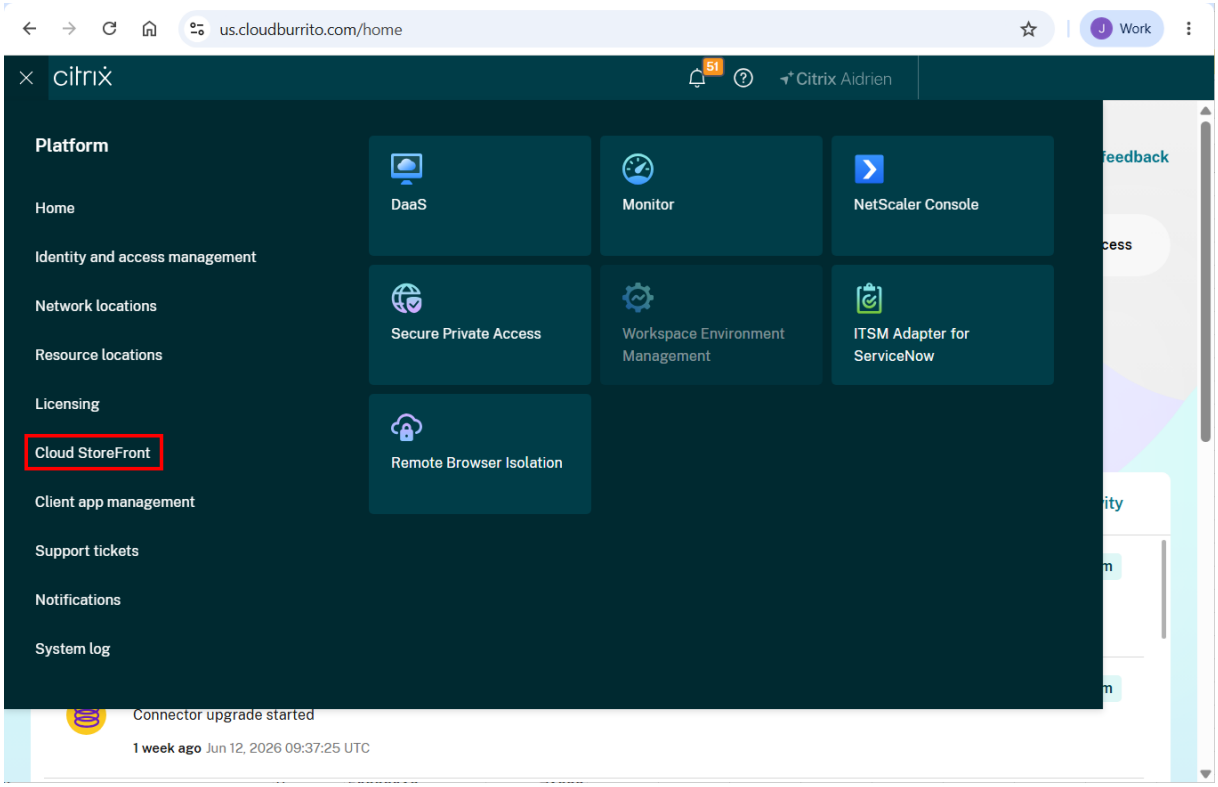
Before using Citrix® StoreFront Cloud you must have completed the following.

- Review the system requirements.
- Have a Citrix Cloud account. For more information, see Signing up for Citrix Cloud.
- Have an Citrix Cloud administrator account with the role **StoreFront Cloud**. For more information, see Add administrators who can configure store.
- Set up at least one service to be accessed from Citrix® StoreFront Cloud. For example:
  - Citrix DaaS Get started: Plan and build a deployment.
  - Secure Private Access onboarding and set up
  - Get started with Remote Browser Isolation.
  - Connect an existing on-premise Citrix Virtual Apps and Desktops site using on-premise site aggregation.

### Step 2: Configure end-user access and authentication

Once you logged into Citrix Cloud, you can access **StoreFront Cloud** from the main menu.




If you do not see this option then ensure you have the **StoreFront Cloud** permission, see Modify administrator permissions.

This step involves configuring access controls, including the authentication methods, the store URL and external connectivity to resources.

> **Note:**
>
> There are two ways for users to access their store. One is through the natively installed Citrix Workspace app for simple, secure access to Citrix Cloud services and stores. The other way to access Citrix® StoreFront Cloud is through a web browser. For more information, see User access.

### Configure store access

You must choose what URL(s) your users use to access their store. By default Citrix® StoreFront Cloud generates a cloud URL based on your customer id but you can change this or add a custom URL from a domain that you own. For more information, see Configure store url.

### Configure authentication to stores

Defining how end-users authenticate to sign in to their stores is a two-step process:

1. Under **Identity and Access Management**, configure Identity and access management.

2. Under **StoreFront Cloud > Authentication**, choose one of the authentication methods delivered by the identity providers you configured in the first step. For more information, see Configure authentication.

If you're using a federated identity provider, you can also enable single sign-on (SSO) to VDAs with the Citrix Federated Authentication Service (FAS).

#### Configure remote access to virtual apps and desktops

By default users must be able to reach their virtual apps and desktops directly over the network. You can configure Citrix Gateway server, or a NetScaler gateway, to allow remote access to your virtual apps and desktops. For more information, see External connectivity.

### Step 3: Customize stores

You can customize the experience of stores for different users and to meet specific organizational requirements in **StoreFront Cloud**, for example:

- The appearance of stores, including logos and colors.
- Interaction options, such as allowing users to create **Favorites** and automatically launching desktops.
- Privacy and security settings. This includes setting a timeout period, creating a sign-in policy, and allowing users to change their passwords from within their stores.

For more information, see Customize store experience.

### Step 4: Configure store resiliency and optimization

For information on improving the efficiency and availability of your DaaS through Citrix® StoreFront Cloud, visit Optimize DaaS in Citrix® StoreFront Cloud. This includes information on how to:

- Optimize connectivity with Direct Workload Connection.
- Ensure service continuity during an outage for offline resilience.
- Configure single sign-on (SSO) to virtual apps and desktops with Citrix Federated Authentication Service (FAS).

### Step 5: Roll out Citrix® StoreFront Cloud to end-users

The broad activities for this step include:

1. Testing stores.

- Verify that you can log in through the browser and into the Citrix Workspace app.
- Launch and use all available apps and desktops.
- Check that customizations such as branding and announcements are dispalyed as expected.
- Check that notifications are displaying the expected actions and activities.

2. Onboarding users.

   - Communicate Citrix® StoreFront Cloud capabilities with users.
   - Share the store URL.
   - Guide users to install the Citrix Workspace app.

## System Requirements

June 22, 2026

### Citrix Cloud™

To configure Citrix® StoreFront Cloud, you must have an account on Citrix Cloud and have enabled either Citrix Desktops as a Service or Secure Private access.

See Citrix Cloud System and Connectivity Requirements

### DaaS

To access DaaS resources, see DaaS system requirements.

### End user connectivity

#### Citrix Workspace™ app

End users can use any supported version of Citrix Workspace app to connect to your store. Older versions of Citrix Workspace app may work but are not supported. It is recommended you use the latest version of Citrix Workspace app. Not all features are available on earlier versions of Citrix Workspace app. For more information about supported features in Citrix Workspace app by platform, refer to the Citrix Workspace app feature matrix.

Citrix Receiver has reached End of Life (EoL). It may work with reduced functionality but is no longer supported. At a minimum, Citrix® StoreFront Cloud requires a version of Citrix Receiver that supports TLS 1.2:

| Receiver | Minimum Version |
|---|---|
| Windows | 4.2.1000 |
| Mac | 12.0 |
| Linux | 13.2 |
| Android | 3.7 |
| iOS | 7.0 |

If you need to use older versions of Citrix Receiver then use Citrix StoreFront which can be configured to allow older TLS versions (not recommended).

#### Web browsers

End users can use the latest versions of the following browsers to connect to their store:

- Microsoft Edge
- Google Chrome
- Mozilla FireFox
- Apple Safari

Admins can use these web browsers to configure Citrix® StoreFront Cloud.

**Citrix® web extensions** For improved experience and reliability, it is recommended that users add Citrix web extension to their web browser. For more information, see Citrix web extension and Install Citrix web extension.

#### Network connectivity

For information about network connectivity, see Citrix Workspace app connectivity in the Citrix Cloud documentation.

### Citrix Virtual Apps and Desktops™ site aggregation

Site aggregation can be used with all supported versions of Citrix Virtual Apps and Desktops. Earlier end of life (EoL) versions of Citrix Virtual Apps and Desktops may work but are not supported.

### NetScaler® Gateway

Citrix® StoreFront Cloud can use any supported version of NetScaler Gateway to provide access to resources. Alternatively use Citrix Gateway Service for a zero deployment solution.

### Federated Authentication Services (FAS)

Citrix® StoreFront Cloud can use FAS to provide single sign-on to resources. For more information, see FAS system requirements.

## User Access

June 22, 2026

Two different methods are available for users to access stores.

- Citrix Workspace™ app - Users with compatible versions of Citrix Workspace app can access their store within the Citrix Workspace app. This provides the best user experience and the greatest functionality.
- Web browser - Users with compatible web browsers can access store by browsing to the store's URL. By default, users also require a compatible version of Citrix Workspace app to open virtual desktops and applications, known as hybrid launch. However, you can configure your website to enable users to access their resources through their browser without installing Citrix Workspace app.

### Citrix Workspace app

Citrix Workspace app is a locally installed app for accessing stores. For more information, see Citrix Workspace app.

Citrix Workspace app offers the following advantages compared with using a web browser:

- **Enhanced security** as it ensures users never download `.ica` files.
- **Enhanced reliability** for opening apps and desktops, as it doesn't rely on client detection.
- **In-built App Protection service** provides an additional layer of security to protect against key-logging and screen-capturing malware.
- **No dependency** on the Citrix web extension.
- **No browser compatibility checks**. As the native app has no dependency on browsers, there's need for browser compatibility checks, unlike the store web client.

- **Better telemetry** because the native app offers extensive information for monitoring purposes.
- **Enhanced HDX™ capabilities** with enhanced features such as optimized codec compression and efficient audio-video compression. These improvements provide high quality and performance for tasks involving high-definition content or graphics-intensive apps.

#### Require use of Citrix Workspace app

You can configure Citrix® StoreFront Cloud so that when users open a store website in their browser, it automatically opens and does not allow users to continue in their web browser. If Citrix Workspace app is not detected then the website gives the user the option to install it. For more information, see Require use of Citrix Workspace app.

#### Configure Citrix Workspace app

After installation, Citrix Workspace app must be configured with connection details for the stores providing users' desktops and applications. You can make the configuration process easier for your users by providing them with the required information in one of the following ways.

**Manual configuration** Users can enter the store URLs into Citrix Workspace app. For more information, see the Citrix Workspace app documentation.

#### Automatic configuration by website

If you have required use of Citrix Workspace app then when the user opens the store URL in their website it automatically configures Citrix Workspace app.

**Provisioning files** After users sign into the store using a web browser, they can go to **Account Settings**, **Advanced** and download a configuration file. When the user opens this file with Citrix Workspace app it adds the store to the app.

**Global App Configuration Service** Use the Global App Configuration Service to configure Citrix Workspace app for your store. See Configure settings for cloud stores.

#### Supported versions of Citrix Workspace app and Citrix Receiver™

For more information on supported versions of Citrix Workspace app and Citrix Receiver, see system requirements.

### Web browser

As an alternative to using a locally installed Workspace app, users can access their store through a web browser. For supported browsers, see system requirements.

When users launch their resources from a web browser there are two possibilities:

1. Resources open within locally installed Citrix Workspace app. This is known as a hybrid launch. This gives users the best experience as it takes advantage of full operating system integration. For more details see Hybrid launch
2. Resources open within their web browser. This makes it possible for users to access resources without needing to install any software locally.

The default configuration is that resources always open within the locally installed Citrix Workspace app. You can change the configuration to either always open resources in the browser or to give the user the choice. For more information, see launch virtual apps and desktops.

If the admin selected **Let end users choose** then when the user first opens the store URL in their browser, the user has the option to click **Use Web Browser** to launch resources within their web browser.

### Hybrid Launch

When users first open a store in browser but are configured to launch apps within the locally installed Citrix Workspace app this is known as hybrid launch. There are a number of ways in which the web site can communicate with the locally installed Workspace app to open resources.

#### Citrix® web extensions

The Citrix web extensions are extensions for commonly used web browsers that improve the user experience for detecting the locally installed Citrix Workspace app and launching virtual apps and desktops. Compared to Citrix Workspace launcher, this provides a better user experience.

The first time a user goes to a store URL on a supported platform, it prompts the user to detect the locally installed Workspace app. It first tries to use the web extension and if this fails then it tries Citrix Workspace Launcher. Existing users who have already completed Workspace app detection can go to **Account Settings**, click **Change Citrix Workspace app** to re-detect workspace app.

#### Citrix Workspace launcher

Citrix Workspace launcher is a component of Citrix Workspace app that allows a store website to detect Citrix Workspace app and launch virtual apps and desktops without requiring an `.ICA` file down-

load. It registers the protocol `receiver` and uses this to communicate with Citrix Workspace app.

When the user first goes to a store URL a supported operating system and browser and Citrix Web Extensions is not installed, it attempts to invoke the Citrix Workspace Launcher using a URL starting `receiver://`. For more information about the user experience, see Citrix Workspace app detection.

When Citrix Workspace Launcher detects a supported version of Citrix Workspace app, it notifies Citrix® StoreFront Cloud. The browser remembers this and uses Citrix Workspace Launcher when launching apps.

The store website invokes Citrix Workspace Launcher when you use the following browsers:

- Firefox 52 or higher
- Chrome 42 or higher
- Safari 12 or higher
- Edge 25 or higher

For managed web browsers, it is recommended that you configure the browser to automatically accept the `receiver` protocol to avoid any prompts.

- On Microsoft Edge, you can use the policy AutoLaunchProtocolsComponentEnabled.
- On Chrome Enterprise, you can use the policy Auto Launch Protocols From Origins.
- On Firefox, you can use the policy AutoLaunchProtocolsFromOrigins.

Citrix Workspace Launcher requires the following minimum versions of Citrix Workspace app or Citrix Receiver.

- Any version of Citrix Workspace app for Windows with the WebHelper component (this is installed by default) or Citrix Receiver for Windows 4.3 or higher.
- Any version of Citrix Workspace app for Mac or Citrix Receiver for Mac 12.0 or higher.
- Citrix Workspace app for Linux 2003 or higher.
- Citrix Workspace app for iOS 2503 or higher.
- Citrix Workspace app for Android 2503 or higher.

If Citrix Workspace launcher is not available, or the user does not allow it to open, then it will not be able to detect the locally installed Citrix Workspace app. The user has the option to try again, or to click **Skip detection**, in which case it falls back to launching apps using `.ica` files. The user can later try again by going to the advanced settings screen and clicking **Verify connection**.

#### ICA file downloads

Where Citrix Web extension and Citrix Workspace launcher are not available, or fail to detect Citrix Workspace app, when a user launches an app or desktop it downloads a `.ICA` file that the user can open with Citrix Workspace app.

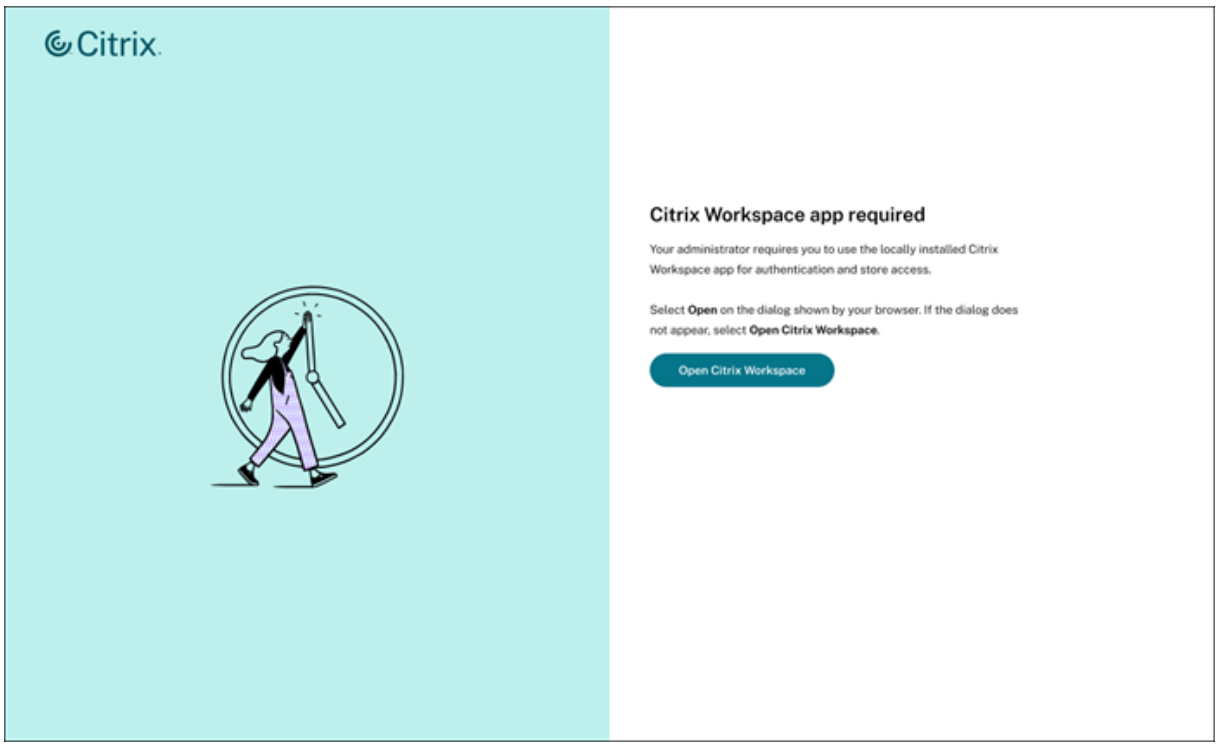
This scenario should be avoided where possible due to the security risks associated with storing ica files on disk. You can configure the website to prevent ICA downloads.

## Require Citrix Workspace app

June 22, 2026

Once administrators have enabled Require Citrix Workspace app, end users can't use the Citrix store web client in browsers.

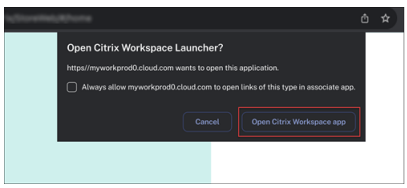
When users try to access web client by entering a store URL in a browser, they see the following web-page that prompts to open the native app.




1. Click **Open Citrix Workspace**.

   The client detection process starts, checking whether Citrix Workspace app is installed locally on the user device.

   The **Open Citrix Workspace Launcher** prompt appears asking users to open the native app.

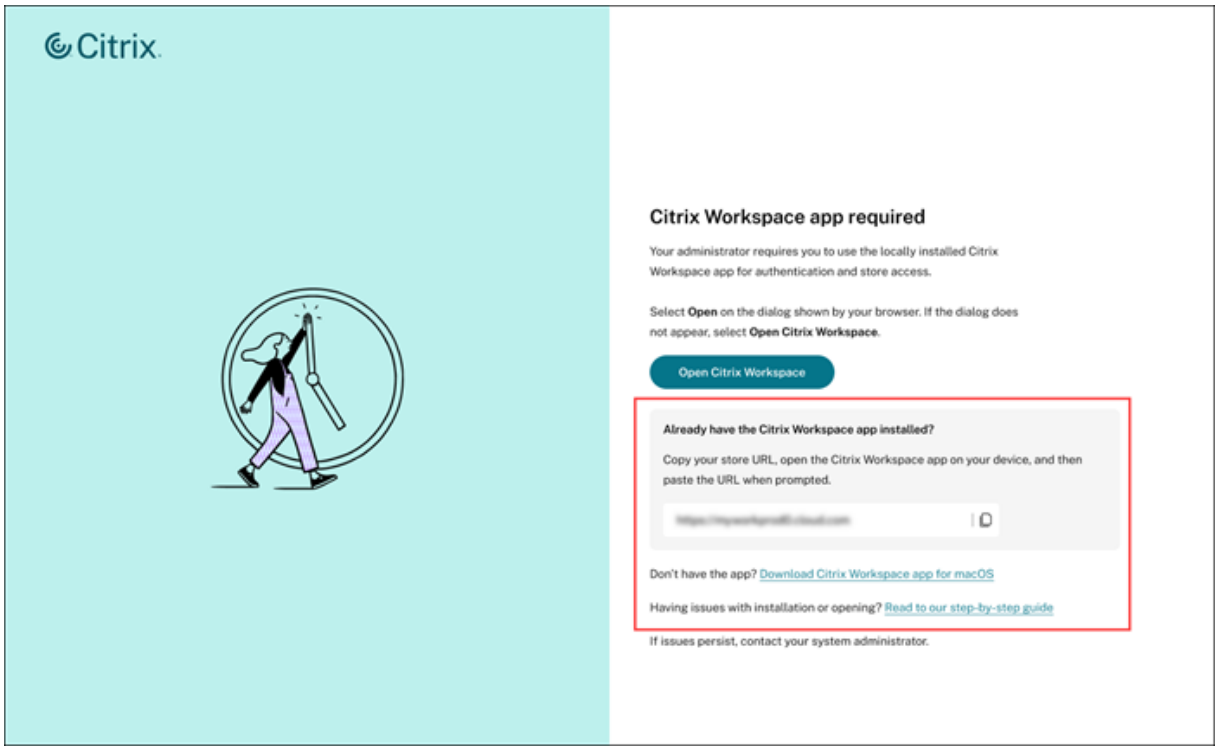


2. Click **Open Citrix Workspace app**.

If a user doesn't see the prompt or doesn't click **Open Citrix Workspace app** on the prompt within 5 seconds, the webpage provides the following extra options to continue:

- The store URL to copy and add manually in the native Citrix Workspace app.
- A download link to install Citrix Workspace app. The behavior of this link depends on configuration.
- The link to the end-user guide, which provides step-by-step instructions for installing and opening Citrix Workspace app.




> **Note:**
>
> If a user is using the Safari browser on an iPad, the browser can't differentiate it from a Mac desktop. Therefore, the user has to click the **I am on iPad** link to proceed with automatic store addition.
>
> Automatic store addition is not supported on Linux and ChromeOS. As a result, the **Open Citrix Workspace Launcher** prompt doesn't appear on these devices. In such cases, users need to manually add the store url in the native app. For more information, see Manual store addition.

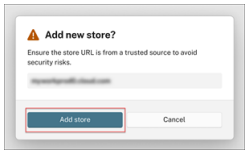
### Automatic store addition

On supported versions of Citrix Workspace app, it automatically adds the store. The minimum versions are as follows:

| Operating system | Compatible version |
|---|---|
| Windows | 24.9.0 or later |
| Mac | 24.5.0 or later |
| Android and iOS | 24.9.0 or later |

> **Note:**
>
> Automatic store addition is not supported on Linux and ChromeOS platforms and has version requirement on Windows and Mac platforms. In such cases, users need to manually add the store url in the native app. For more information, see Manual store addition.



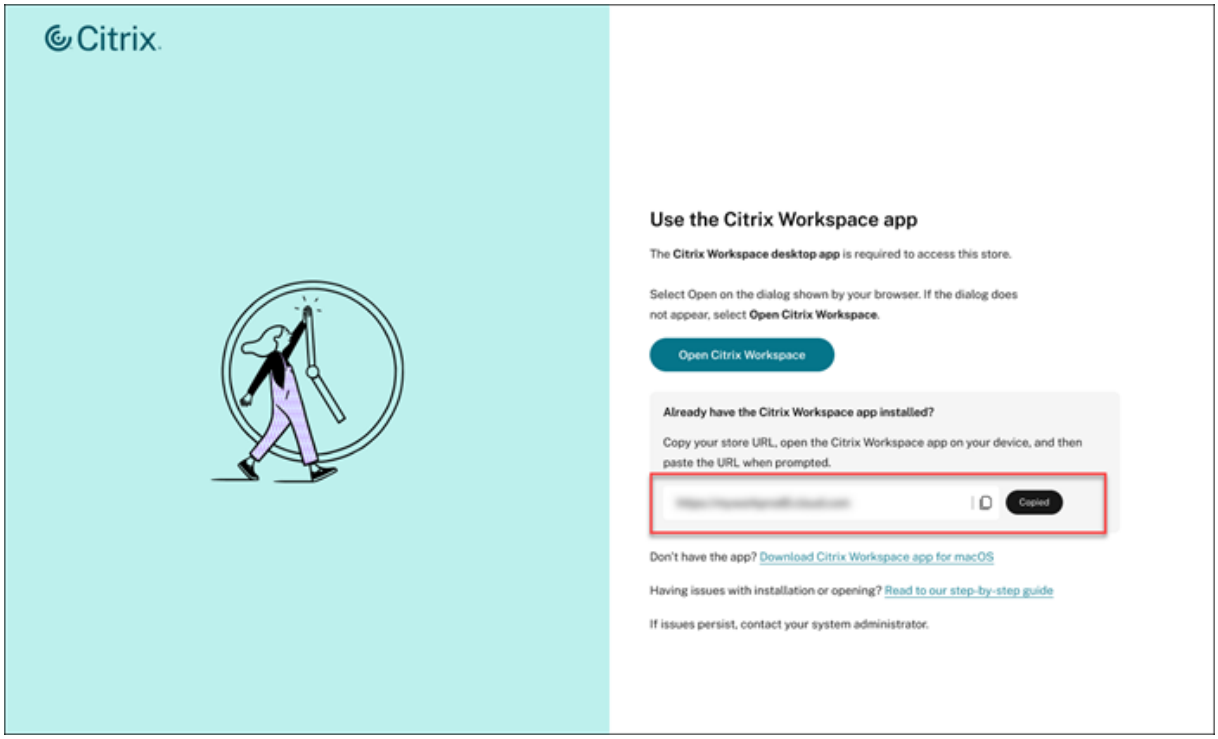

Click **Add store**.

Once clicked, the native app automatically captures the store URL entered in the browser and displays the authentication page for the user to sign in. After the successful authentication, the user can see the home page of the native Citrix Workspace app.

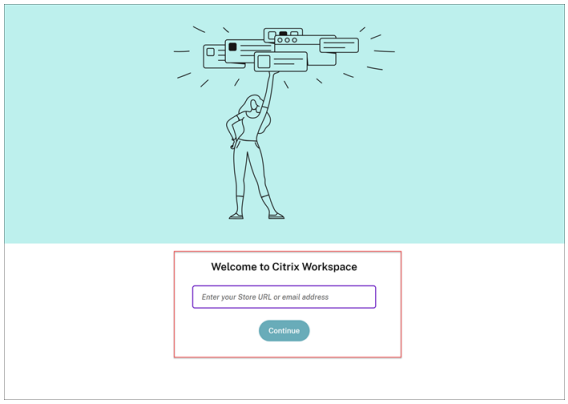
### Manual store addition

Users can manually add a store to Citrix Workspace app if the native app doesn't automatically capture the store URL when they click the **Add store** option.




1. Copy the store URL from the native mandate webpage, and paste it into the **Welcome to Citrix Workspace** page.




2. Click **Continue**.

After submitting a valid store URL, Citrix Workspace app displays the authentication page for the user to sign in. After the successful authentication, the user can see the home page of the native Citrix Workspace app.

## Citrix Workspace app detection

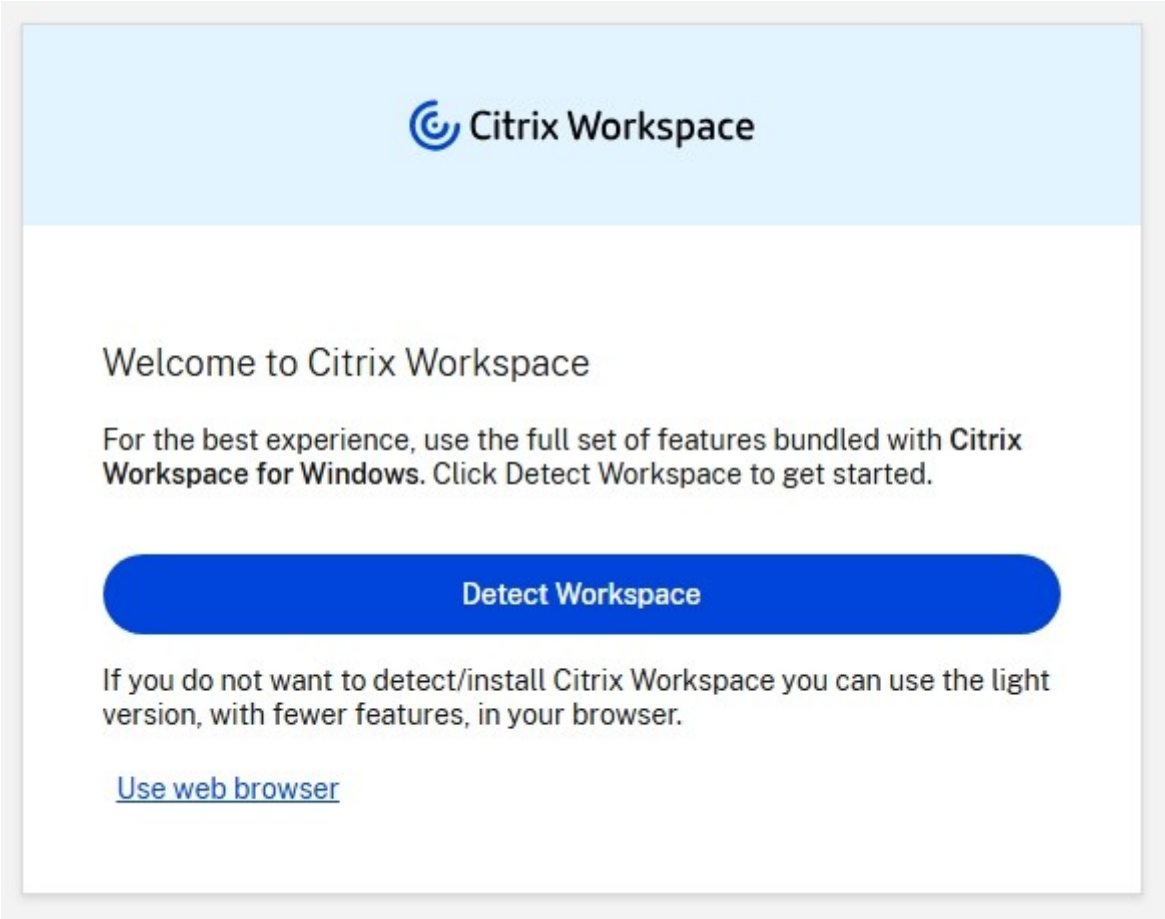
June 22, 2026

### Welcome screen

When accessing the store through a web browser, the website may display the **Welcome** screen. This applies when:

- The user opens the store in their web browser for the first time, or after clearing site data from the web browser.
- Launch virtual apps and desktops is set to **Open in Citrix Workspace app** or **Let the user choose**.
- If Citrix Web Extension is not installed, or has not detected Citrix Workspace app. If Citrix Web Extension detects Citrix Workspace app then it skips this step and defaults to launching in Citrix Workspace app.
- The device's operating system supports Citrix Workspace launcher.



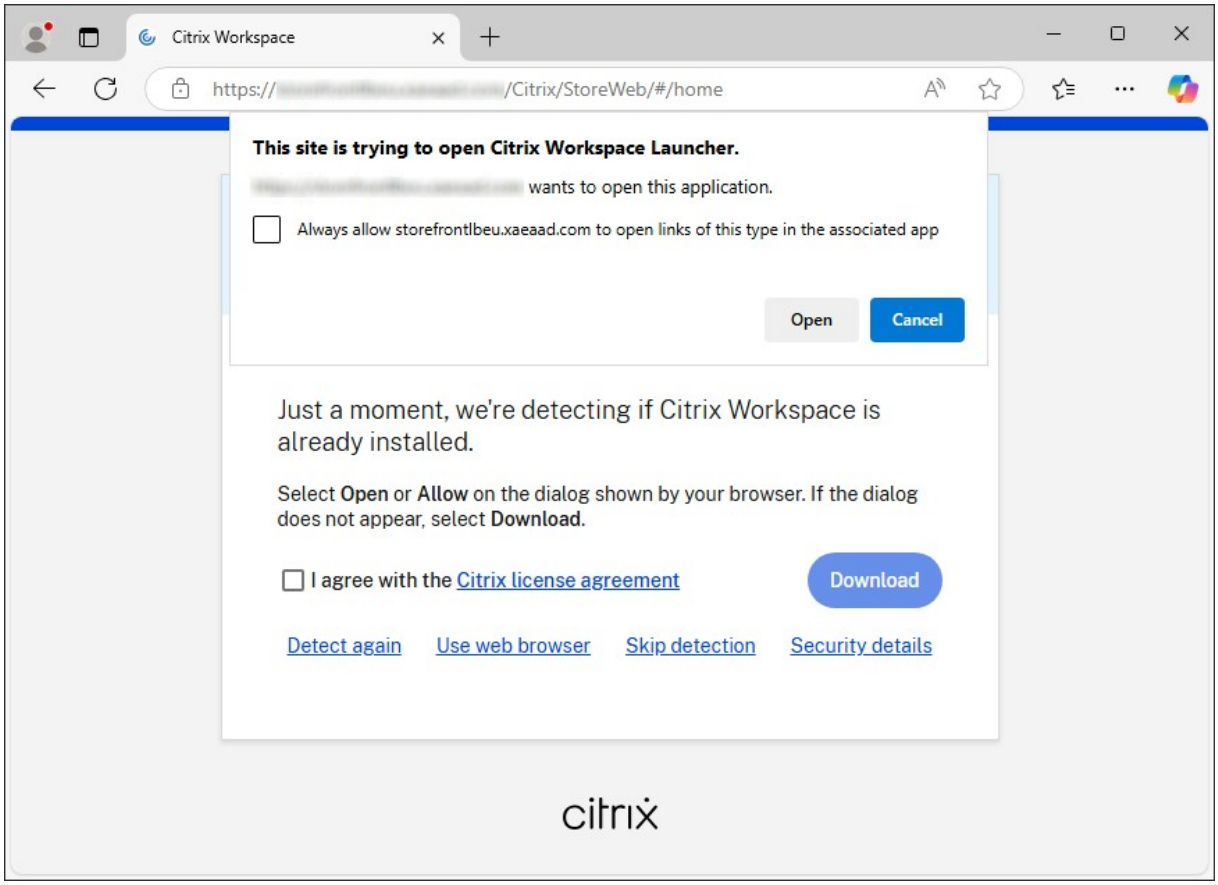

Users can either:

- Select **Detect Citrix Workspace app** if they wish to launch resources in the locally installed Citrix Workspace app. This is recommended for the best experience.
- Select **Use web browser** to always launch resources within the browser. This option is only available if Launch virtual apps and desktops is set to **Let the user choose**.

### Citrix Workspace app detection screen

When the user selects **Detect Citrix Workspace app**, the website displays the Citrix Workspace app detection screen. The screen attempts to open **Citrix Workspace Launcher** which is a component of Citrix Workspace app. If the user has installed Citrix Workspace app then the browser may display a message asking to run the **Citrix Workspace Launcher**. The user must select **Open Citrix Workspace Launcher**, **Open link**, **Open**, or **Always open** (depending on the browser). Citrix recommends that users also select **Always allow *domain* to open links of this type in the associated app** (or similar depending on the browser) to avoid this message appearing every time they launch a resource. You can configure managed browsers to always open **Citrix Workspace launcher** without any prompts. For more information, see Citrix Workspace launcher.




The user can also reach this screen from the Advanced setting page by selecting **Verify connection**.

If a locally installed Citrix Workspace app is detected then after a few seconds it continues to the next screen. When the user subsequently launches a resource it uses Citrix Workspace Launcher to open resources in the locally installed Citrix Workspace app.

If Citrix Workspace app is not installed, or the user cancels Citrix Workspace launcher then they might have the following options:

- **Download** - Downloads Citrix Workspace app from the Citrix website. To configure this option,

see Configure native app download link for end users.

- **Detect again** - Attempts to detect the locally installed Citrix Workspace app again.
- **Use web browser** - Skips Workspace app detection and always opens resources in the web browser. This option is only available if Launch virtual apps and desktops is set to **Let the user choose**.
- **Skip detection** - Users can use this option if they have a legacy version of Citrix Receiver installed that does not support the Citrix Workspace Launcher or Citrix web extensions. If they select this option, when they launch a virtual app or desktop then their browser downloads a `.ica` file that they can open with Citrix Workspace app. This option results in reduced functionality and security so is not recommended. Administrators can remove this option, for more information, see Prevent ICA downloads.

## Assigned desktop power management

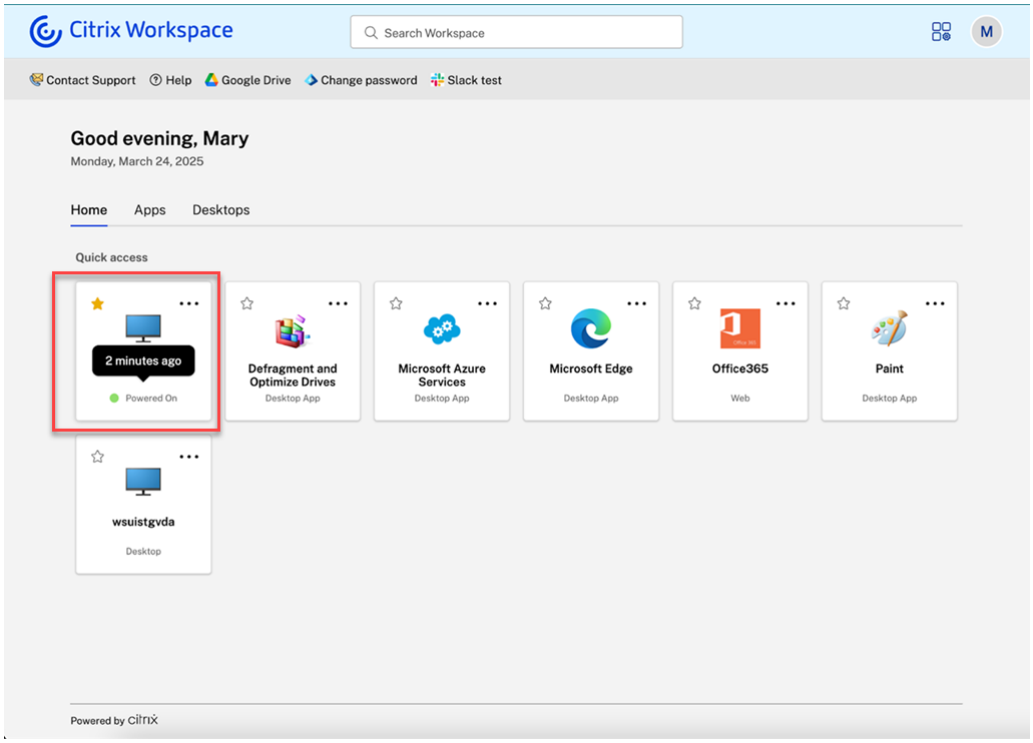
June 22, 2026

### Power status

The desktop tile may displays the power status if:

- The machine catalog has a single-session OS where the Desktop Experience is set to **Connect to the same (static) desktop each time the users log in.**.
- The machine catalogue must be configured as power managed.
- Citrix DaaS or Citrix Virtual Apps™ and Desktops 2511 or later versions publish the machine using site aggregation.




The following power statuses may be displayed:

- **Powered off:** The machine has been shut down and is not currently running.
- **In hibernation:** The machine is in a hibernation state, where its current session is saved to disk, and the machine is using minimal power.
- **Powering on:** A machine that was in the **Powered Off** or **In hibernation** has been recently started but is not yet ready to use.
- **Powered on:** The desktop is running.
- **Ready:** The desktop has registered with the delivery controller and is ready to launch.
- **Shutting down:** The user has initiated a shut down.

The status is refreshed every two minutes or when the user clicks the ellipsis menu on the desktop tile. When the user hovers over the power state it displays when the last refresh occurred.

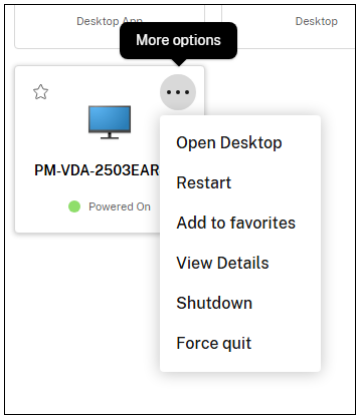
### Known issues

- When you launch one of multiple power-managed desktops, store might show inconsistent power statuses for the other desktops until the first desktop completes launching. [WSUI-10870]

### Power actions

The **More** options menu (ellipsis icon) on the tile provides users with access to relevant actions. For power managed assigned machines there are additional actions that depend on the current power state of the resource.




These actions might include:

- **Open Desktop** - Launch or reconnect to the desktop.
- **Troubleshoot** - Checks for any issues that could cause launch failures.
- **Restart** - Initiates a force restart. Only available for assigned power managed desktops.
- **Log out** - Logs out of the desktop. Only available if the user has a logged in session.
- **Disconnect** - Disconnects from desktop. Only available if the user has an active session.
- **Shut down** - Initiates a graceful shutdown. Only available for assigned power managed desktops.
- **Force shutdown** - Force powers off the machine. Only available for assigned power managed desktops.
- **Hibernate** - Puts the dedicated desktop into a hibernation state. Only available for assigned power managed desktops where hibernation is enabled.
- **Resume** - Wakes the dedicated desktop from a hibernated state. Only available for assigned power managed desktops where hibernation is enabled.

## Activity Manager

June 22, 2026

Activity Manager is a simple yet powerful feature in Citrix® StoreFront Cloud that empowers users to effectively manage their resources. It enhances productivity by facilitating quick actions on active apps and desktops from any device. Users can seamlessly interact with their sessions, ending or dis-

connecting sessions that are no longer required, freeing up resources and optimizing performance on the go.

The Activity Manager panel displays a consolidated list of apps and desktops that are active not only on the current device but also on any remote device that has active sessions. Users can view this list by clicking the Activity Manager icon located next to the profile icon on desktop and at the bottom of their screen on mobile devices.

> **Note:**
>
> If you are unable to view the Activity Manager icon in a darker banner theme, consider changing and testing the color selected in the **Banner text and icon color** setting. The icon might not be visible clearly due to a low contrast between the banner and the Activity Manager icon. For more information, see Configure custom themes.

### Enable Activity Manager and power management controls

The Activity Manager feature is enabled by default.

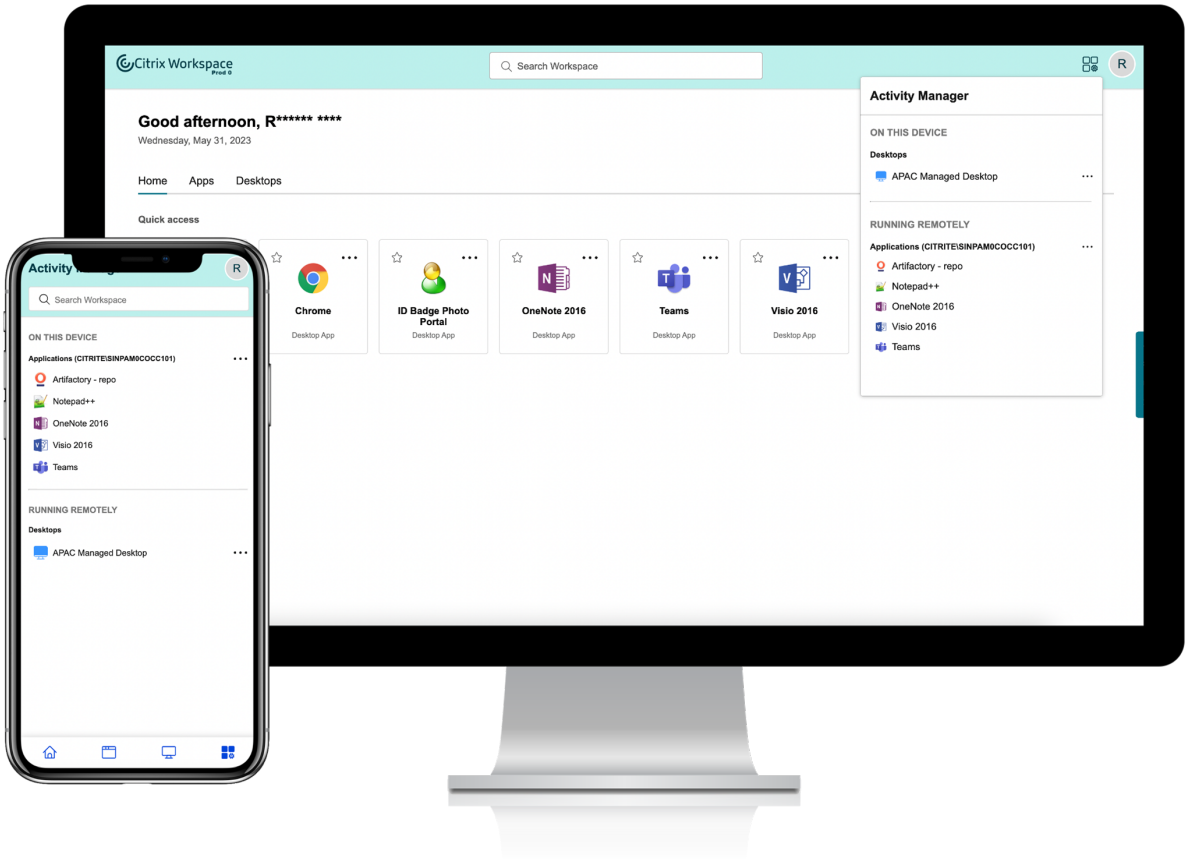
You can enable power management controls from the Features screen.

### Using Activity Manager

Active apps and desktops are grouped as follows on Activity Manager.

- A list of apps and desktops that are active on current device are grouped under **On this device**.
- A list of apps and desktops that are active on other devices are grouped under **Running Remotely**.




Users can perform the following actions on an app or desktop by clicking the respective ellipsis(…) button.

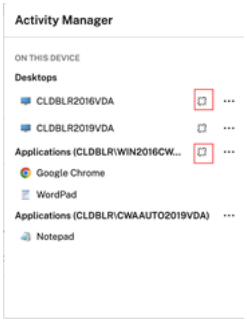
- **Disconnect**: The remote session is disconnected but the apps and desktops are active in the background.
- **Log out**: Logs out from the current session. All the apps in the sessions are closed, and any unsaved files are lost.
- **Shut Down**: Closes your disconnected desktops.
- **Force shutdown**: Forcefully powers off your desktop in case of a technical issue.
- **Restart**: Shuts down your desktop and start it again.
- **Hibernate**: Saves the current state and powers off the machine.
- **Resume**: Starts and restores the state of a machine in hibernation state.

### Disconnected apps and desktops

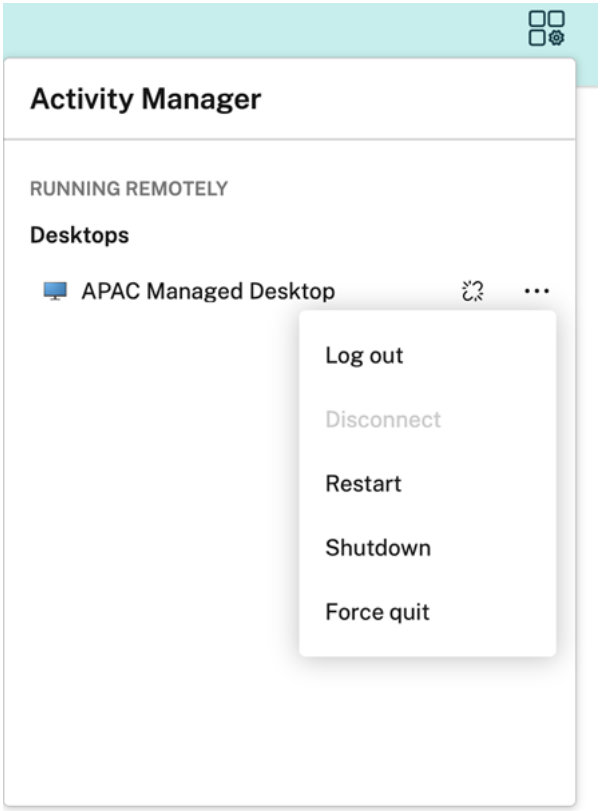
Activity Manager enables end users to view and take actions on apps and desktops that are running in disconnected mode, locally or remotely. Sessions can be managed from mobile or desktop devices,

enabling end users to take action on the go. Taking action on disconnected sessions such as log out or shut down promotes optimized use of resources and reduces energy consumption.




- The disconnected apps and desktops are displayed on the Activity Manager panel and are indicated by a disconnected icon.
- The disconnected apps are grouped under the respective sessions and the sessions are indicated by a disconnected icon.




End users can take the following actions on their disconnected desktops by clicking the ellipses button:

- **Log out**: use this to log out from your disconnected desktop. All the apps in the session are closed, and any unsaved files are lost.

- **Shut Down**: use this option to close your disconnected desktops.
- **Power off**: use this option to forcefully power off your disconnected desktops in case of a technical issue.
- **Restart**: use this option to shutdown and start the disconnected desktop again.

The behavior of disconnected sessions on Activity Manager differs as follows.

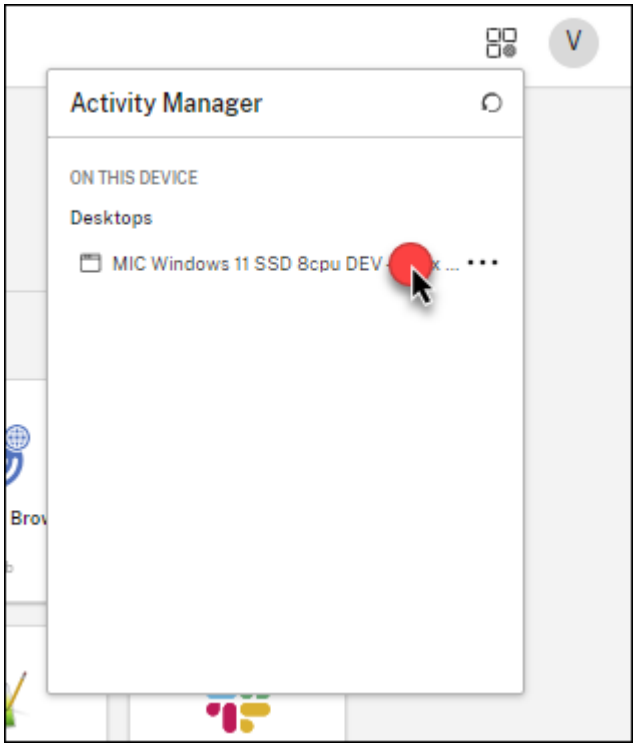
- If the user is signed into a store through a browser, and disconnects a local session, the session is first displayed under **On this device**. However, once the user closes and reopens Activity Manager, the disconnected session is moved under Running Remotely.
- If the user is signed into Citrix Workspace app, and disconnects a local session, the disconnected session disappears from the list. However, once the user closes and reopens Activity Manager again, the disconnected session is moved under **Running Remotely**.

### Reconnect to disconnected apps and desktops

The reconnect feature allows end users to effortlessly reopen their disconnected apps and desktop sessions, ensuring a smooth transition between devices without losing progress. This feature seamlessly restores access to the previous work environment, eliminating the need to search for and reopen apps and desktops.

To reconnect to a disconnected app or desktop:

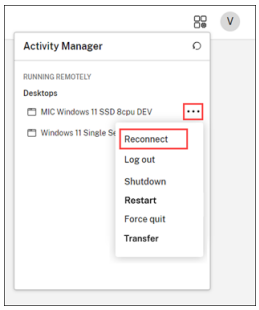
- Open Activity Manager and then click on the resource item.



OR

- Click the ellipsis button (...) and then click **Reconnect**.

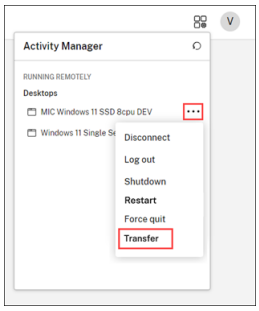



Clicking **Reconnect** reopens the disconnected resource from where you left off.

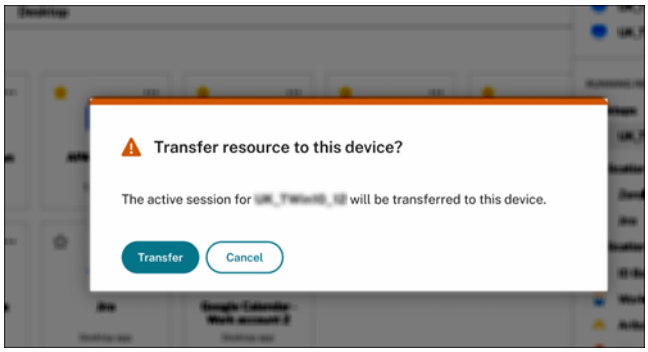
### Transfer your apps and desktops

The transfer feature allows end users to transfer their active apps and desktop from other devices to the current device. To transfer the apps and desktops, follow these steps:

1. Click the ellipsis button (...) and then click **Transfer**.

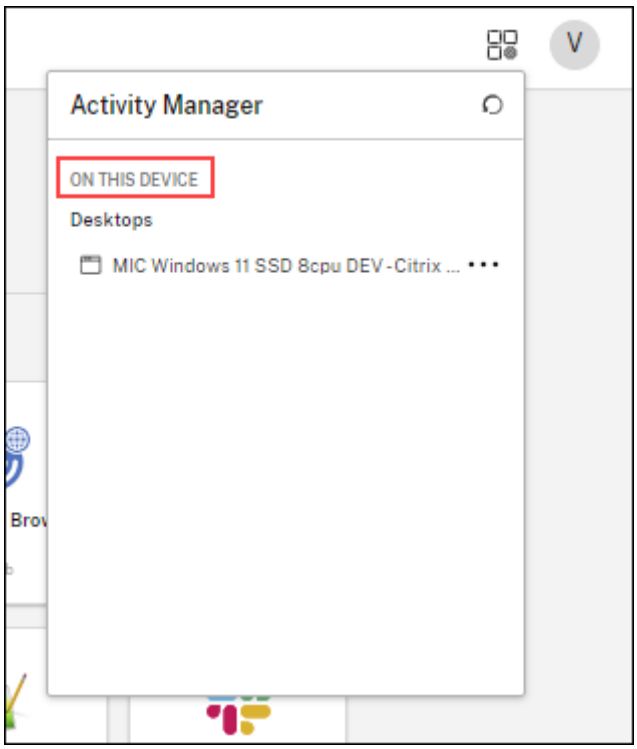



2. Click **Transfer** on the confirmation dialog box.




Once the resources are transferred to the current device, you can see them listed under the **ON THIS DEVICE** section in the Activity Manager.




### Hibernate and Resume virtual desktop sessions

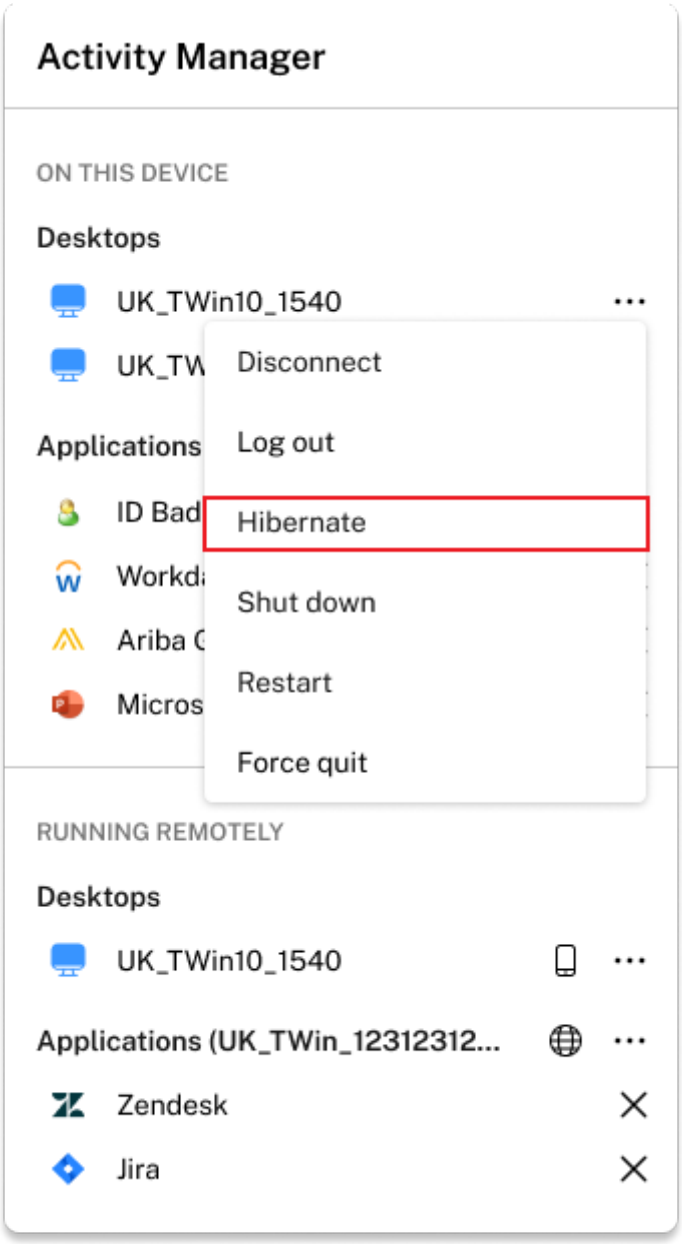
The Hibernate and Resume feature allows users to optimize resource utilization by hibernating virtual desktops when not in use and seamlessly resuming them as needed. This not only saves costs and energy but also enhances user workflow with faster session resumption times.

When initiating hibernation, the hypervisor communicates with the guest operating system, triggering a suspend-to-disk action. During this process, the memory (RAM) contents of the virtual desktops are preserved on the OS disk, while the virtual desktop itself is deallocated. Upon subsequent startup, the virtual desktop's RAM contents are restored from the OS disk, ensuring that applications and processes resume seamlessly from their last state.

Hibernation is available for assigned power managed desktops on supported hypervisors. To enable hibernation capability, an administrator needs to follow specific guidelines and enable preview features both in Azure and Citrix DaaS. For more information, see Create hibernation-capable VMs (Preview).

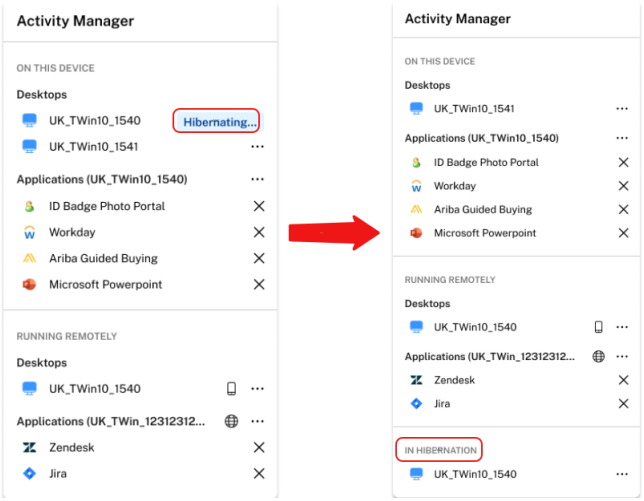
**Hibernate a desktop session:**



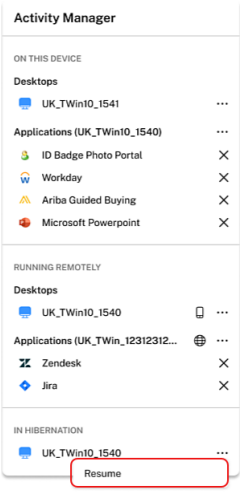

To hibernate a desktop session, users can click the three-dot button (**...**) and then click the **Hibernate** option. The desktop initiates the hibernation once the users click the **Hibernate** option. Once the desktop is hibernated, the desktop resource moves to the **In Hibernation** section on **Activity Manager**.



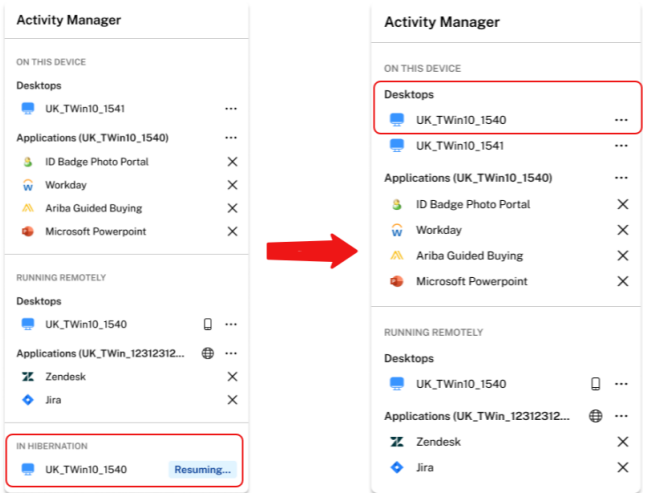

**Resume a hibernated desktop session:**

Hibernated desktop sessions are available under the **In Hibernation** section on **Activity Manager**. To resume the hibernated desktop session, users can click the three-dot button (...), and then click the **Resume** option.




Once users click the **Resume** option, the desktop gets restored.




## Citrix web extension

June 22, 2026

Citrix web extension establishes a secure and reliable connection between the store website and the locally installed Citrix Workspace app. It streamlines the opening of apps and desktops from the web client to the native app, which uses HDX™ protocol. When you access the web client and open any apps or desktops after installing this extension on your browser, the extension opens the app or desktop from your native Citrix Workspace app.

The web extension offers various benefits such as seamless opening of desktop and apps, service continuity, supports App Protection service etc. For more information on the benefits of the web extension, see Benefits of Citrix web extension. To find out what's new, see What's new

> **Note:**
>
> Users need to have the Citrix Workspace app client natively installed on their device for this extension to work. To download Citrix Workspace app, visit the Citrix Downloads page.

### Supported Browsers

| Browser name | Operating systems | Browser Version |
|---|---|---|
| Google Chrome | Windows, macOS, Linux | Latest |
| Microsoft Edge | Windows, macOS, Linux * | Latest |
| Safari | macOS | Latest |

* Citrix Web Extension only works with Microsoft Edge if Google Chrome is also installed on the device. A future release might address this.

> **Important:**
>
> On Linux, install the browser before you install Citrix Workspace app. If you install the browser after installing Citrix Workspace app, Citrix Web extension does not detect Citrix Workspace app. To resolve this, reinstall Citrix Workspace app.

## Supported versions of StoreFront™

The extension is available for both cloud and on-premises stores.

Citrix web extension is always available for use with Citrix® StoreFront Cloud without requiring any additional configuration.

To use the Citrix web extension with StoreFront, StoreFront 2203 CU2 or higher is required.

- For StoreFront versions earlier than 2402, Citrix web extension is disabled by default and you must enable it manually.
- For StoreFront version 2402, Citrix web extensions is enabled by default for new deployments but you must manually enable it when upgrading from a previous version.
- For StoreFront 2407 and later, Citrix web extension is enabled by default and hence you don't need to do any configuration.

For more information about enabling use of Citrix web extensions in StoreFront, see Citrix web extensions on StoreFront.

## Benefits of Citrix web extension

The web extension enhances the reliability and security of hybrid deployments. It comes with the following built-in features.

### Seamless opening of desktops and apps

Normally, the store website uses Citrix Workspace launcher to detect the locally installed Citrix Workspace app and launch virtual apps and desktops. However, each time the website invokes Citrix Workspace launcher, the browser displays a pop-up asking for permission, unless the user chooses the option to always always allow permission. The web extension allows the web client to seamlessly open desktops and apps with no browser pop-ups.

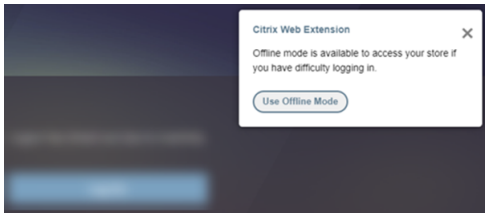
### More reliable launches for StoreFront GSLB deployments

When using multiple StoreFront deployments behind a Global Server Load Balancer (GSLB), the responses might be directed to the wrong server, leading to failures in opening apps and desktops. This can be mitigated through GSLB configuration but it is complex to configure. Citrix web extension allows for reliable client detection and opening of apps and desktops with no special configuration for GSLB deployments.

### Service Continuity for store

If a user is unable to sign in to their store, Service Continuity enables them to open their resources in offline mode. For more information, see Service Continuity.

When accessing the store web client, users must install Citrix web extension to enable service continuity. During the initial sign in, the extension stores connection leases. Subsequently, if sign-in fails after 60 seconds, the web extension displays a prompt to use Offline Mode.




Users can continue their work without losing their data, enhancing work productivity. Once connectivity is restored, users can click **Reconnect to store** to switch to online mode.

> **Note:**
>
> This functionality applies only when using Citrix® StoreFront Cloud, not on-premises StoreFront.
>
> This new offline mode prompt is applicable only to Chrome and Edge browsers. For Safari browser, the old prompt remains unchanged.

### App Protection for store

Citrix® StoreFront Cloud can be configured so that the web extension is required for users to view and open apps that have App Protection enabled. This feature prevents unauthorized access to sensitive information from apps by protecting users from keylogging, screen capturing, and other security threats.

For more information, see Show or hide resources requiring App Protection.

### Install Citrix web extension

For more information on the installation of the web extension, see Install Citrix web extension.

### Reference articles

- Citrix web extensions on StoreFront
- Citrix® StoreFront Cloud product documentation
- Citrix Workspace app product documentation
- Support for browser extensions on Citrix Enterprise Browser
- Service Continuity - Citrix® StoreFront Cloud with DaaS Deployments

## What's new in Citrix Web Extension

June 22, 2026

### 25.7.3

- Citrix web extension now supports service continuity when using a custom domain.
- This release fixes an issue where Citrix web extension does not work on Safari.

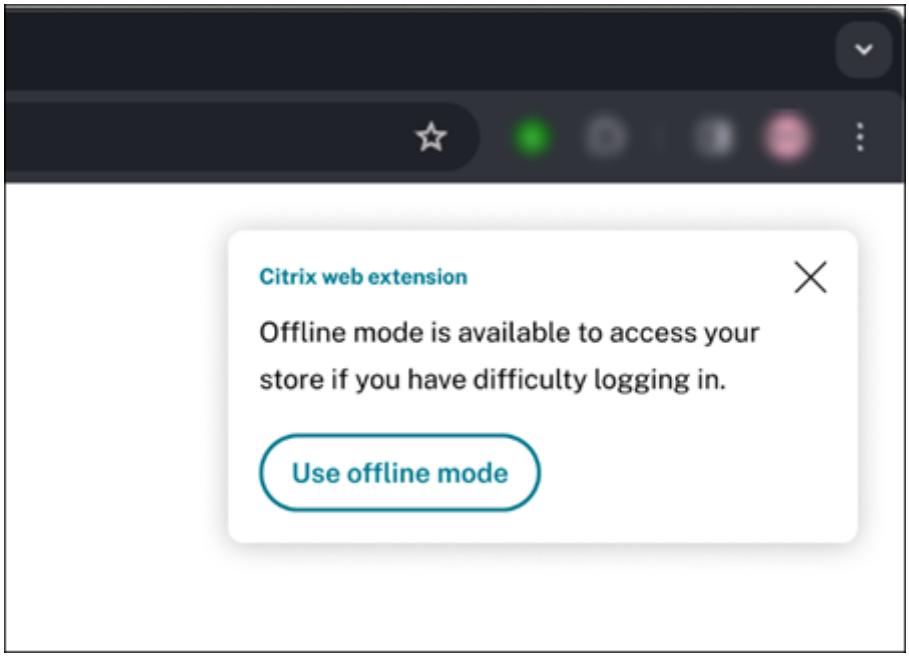
### 24.6.0

#### Store offline mode prompt

The new prompt brings enhancements in the following areas: improved design, enhanced behavior, and loading time.

**Design** The new prompt now appear as a pop-up on the screen. Previously, the prompt appeared as a new page that required the user to either reinitiate the authentication or work offline. However, the new pop-up design doesn't need a mandatory response from a user. It provides an option to the user to choose the offline mode if they encounter any connectivity issues. The new prompt is less intrusive and allows users to continue with their ongoing authentication process.




Additionally, the new prompt is movable, allowing the user to drag it anywhere on the screen to see the content behind it.

**Behavior and loading time** Significant enhancements are made to the behavior and loading time of the offline mode prompt.

**Old behavior:** Previously, the prompt appeared within 30 seconds after the user entered the store URL in the browser. Sometimes it might take some extra time for users to sign in to the store due to reasons such as waiting for a push notification, entering 2-factor authentication code, webpage loading time, etc. If user authentication exceeds the 30-seconds threshold due to these reasons, the prompt would appear, interrupting the authentication process.

The user response to the prompt is mandatory and leaves them with only two options: either switch to offline mode or retry the authentication process. Choosing the retry option required the user to reinitiate the whole process, and they had no option to continue with the ongoing authentication process once the prompt window appears.

**New behavior:** The enhanced offline prompt is less intrusive, as it doesn't interrupt the ongoing user authentication. Users can choose either to continue with the authentication process or can use the offline mode if they are facing any connectivity issues.

The offline mode prompt now appears on the webpage only after 60 seconds, without interrupting the ongoing user authentication process. Due to some reasons if IdP domain fails to respond, the browser doesn't load any page. In such scenarios, a dialog box appears for offline mode instead of the usual pop-up prompt.

### 24.4.0

#### Supports Custom domains

Starting with version 24.4.0, Citrix Web Extension now fully supports the opening of apps and desktops for custom domains on both Microsoft Edge and Google Chrome browsers. Users can seamlessly access their store resources on custom domain URLs, enhancing productivity and streamlining workflows.

## Install Citrix® web extension

June 22, 2026

There are a number of ways to deploy the Citrix web extension.

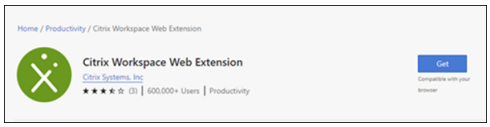
- Manually install from app stores
- Configure store to prompt users to install Citrix web extension
- Using device and web browser management tools.

Once the extension is installed, users can view the detection status and verify whether Citrix web extension is used to launch apps and desktops.

### Manual installation

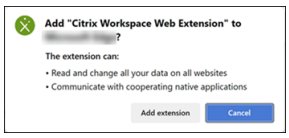
Administrators and end users can add the extension to web browsers manually:

1. Go to the Citrix web extension page in the browser's web store.
    - Chrome web store
    - Microsoft Edge Addons
    - Mac App Store
2. Add the extension.
    - In the Chrome web store press **Add to Chrome**.
    - In Microsoft Edge Addons or the Apple Mac Store press **Get**.



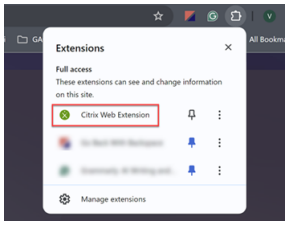

 

3. Confirm the pop-up message to add the extension to the browser with the requested permissions.




> **Note:**
>
> Although it requires permission to read and change data on all websites, it only activates on websites where the URL contains **Citrix**.

Once the extension is added, you can see the extension icon displayed under the **Extensions** button on the toolbar.




For easy access, users can press the pin button to add the extension to the toolbar.

### Prompt users to install Citrix web extension

You can configure store websites to prompt users to install Citrix web extension when they try to launch a resource. It provides a link to the browser web store. Subsequent steps are the same as manual installation.

This functionality is not available on StoreFront.

### Deploy web extension to managed devices and web browsers

Depending on the browser and operating system, you can automatically deploy the Citrix web extensions to devices or web browsers that you manage.

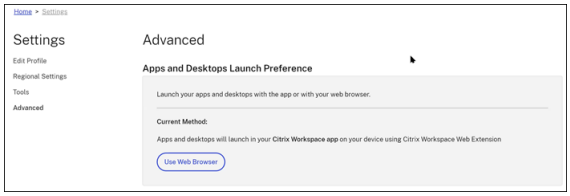
- To deploy Microsoft Edge extensions, see Manage Microsoft Edge extensions in the enterprise.
- To deploy Chrome extensions using Google Admin console, see Automatically install apps and extensions.
- To deploy Google Chrome extensions on Windows using group policy, see Set Chrome app and extension policies (Windows).
- To deploy Chrome extensions on Linux using a configuration file, see Set Chrome app and extension policies (Linux).

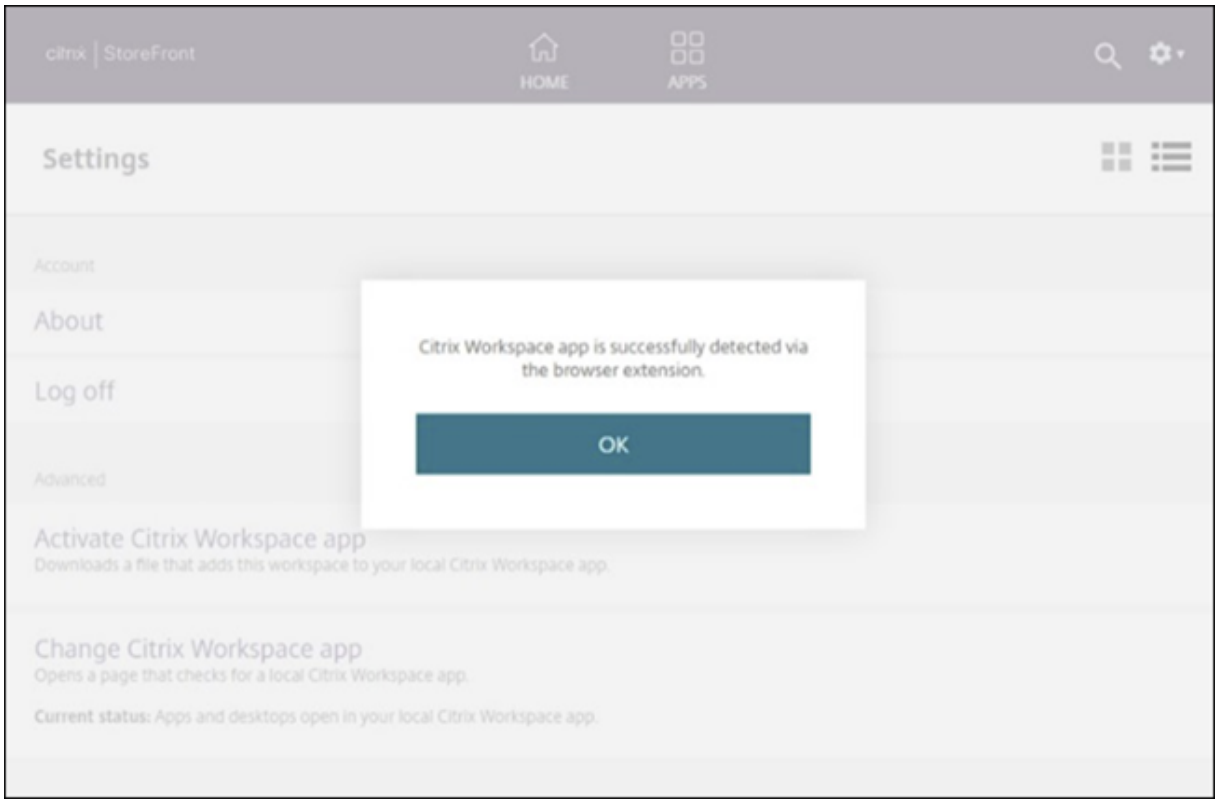
### Verify whether Citrix web extension is used to launch apps and desktops

Once the web extension is added, users can verify whether it is activated and opens apps and desktops in Citrix Workspace app by going to **Settings** > **Advanced**.

On the modern UI, the **Settings** screen displays the message **Apps and desktops will launch in your Citrix Workspace app on your device using Citrix web extension**.



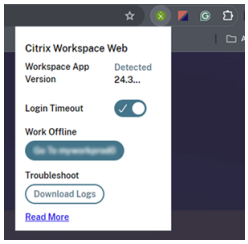

On on-prem StoreFront™ with the Classic UI, click **Change Citrix Workspace app**. If the web extension is detected, it displays the message **Citrix Workspace app is successfully detected via the browser extension**.




### Citrix web extension status

To view the status while on a store website, click on the extension to open it.




It displays the following information and options:

- **Workspace app:** Whether Citrix Workspace app is detected.
- **Version:** The version of Citrix Workspace app detected.
- **Login Timeout:** Manage the offline mode prompt through the Citrix web extension in the browser. To turn off the offline mode prompt, click the extension icon and disable the toggle button.
- **Work Offline:** Manually switch to offline mode without waiting 60 seconds for the offline mode prompt. This option is also useful in the case where **Login Timeout** is disabled.
- **Troubleshoot:** You can collect the error logs using the **Download Logs** option when there are any issues.
- **Read More:** Click this link to learn more.

### Upgrading Citrix web extension

By default, Chrome, Edge and Safari automatically update extensions to the latest version.

## Configure access to stores

June 22, 2026

When you first enable store, a default cloud.com store URL is created to allow users to access the store from their locally installed Citrix Workspace app or web browsers. You can customize this URL or add additional URLs. For more information, see store URL in this article.

For information on how users can connect to their stores, see User access options.

To configure how users authenticate to their store, see Configure Authentication.

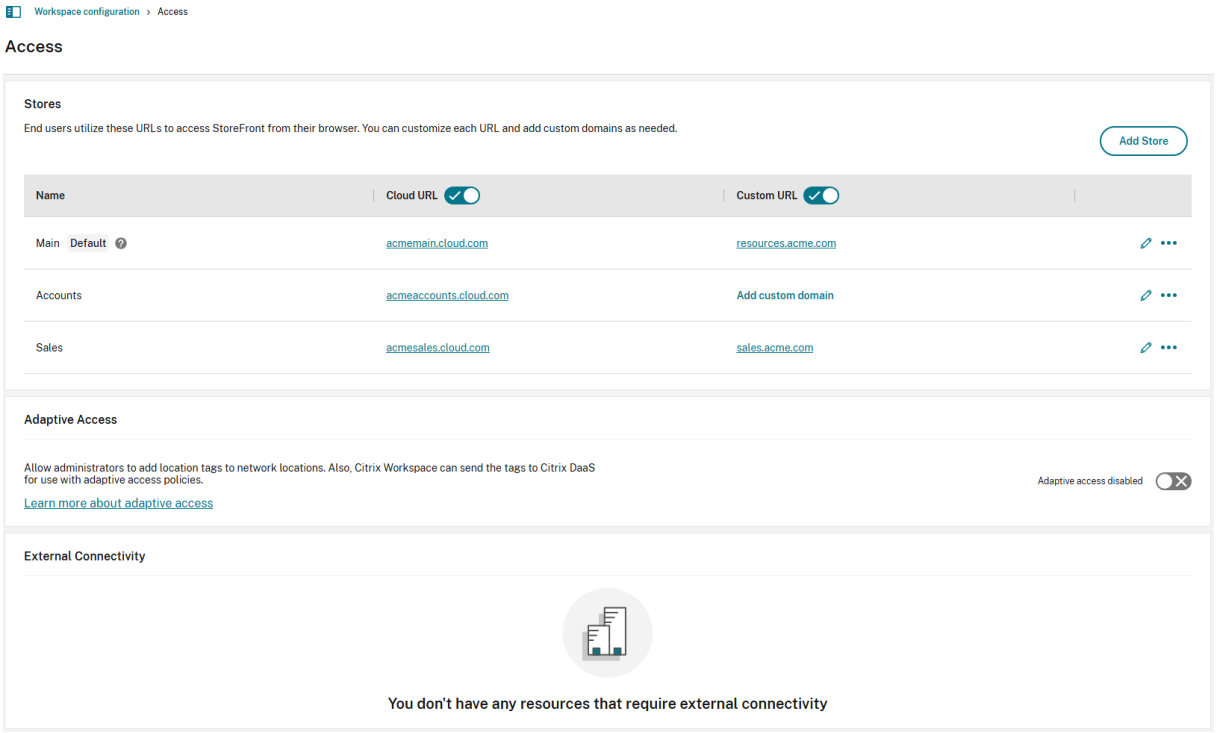
When a user launches a resource, the user's device must be able to reach the Virtual Delivery Agent (VDA). For internal users, the endpoint must connect directly to the IP address of the Virtual Delivery

Agent (VDA). Remote users can gain external access to their resources if you configure external connectivity with Citrix Gateway or the Citrix Gateway service. For information on enabling remote access to stores, see External connectivity in this article.

To configure access settings:

1. Go to Citrix Cloud™ and sign in with your credentials.
2. Navigate to **StoreFront Cloud** > **Access**.




## Store URL

To configure the cloud.com URLs that your end users use to access their store, see Configure store URLs.

## Custom store URL

In addition to the cloud.com store URLs, you can use your own custom URLs linked to your store URLs. For more information, see Configure a custom domain.

## Adaptive Access

The Adaptive access feature enables admins to provide granular level access to the apps that users can access based on the context. For more information, see Adaptive access.

To enable Adaptive Access

1. Go to the **Access** tab.
2. Go to the section **Adaptive access** and click the toggle. A confirmation screen appears.
3. Press **Enable**.

To disable Adaptive Access:

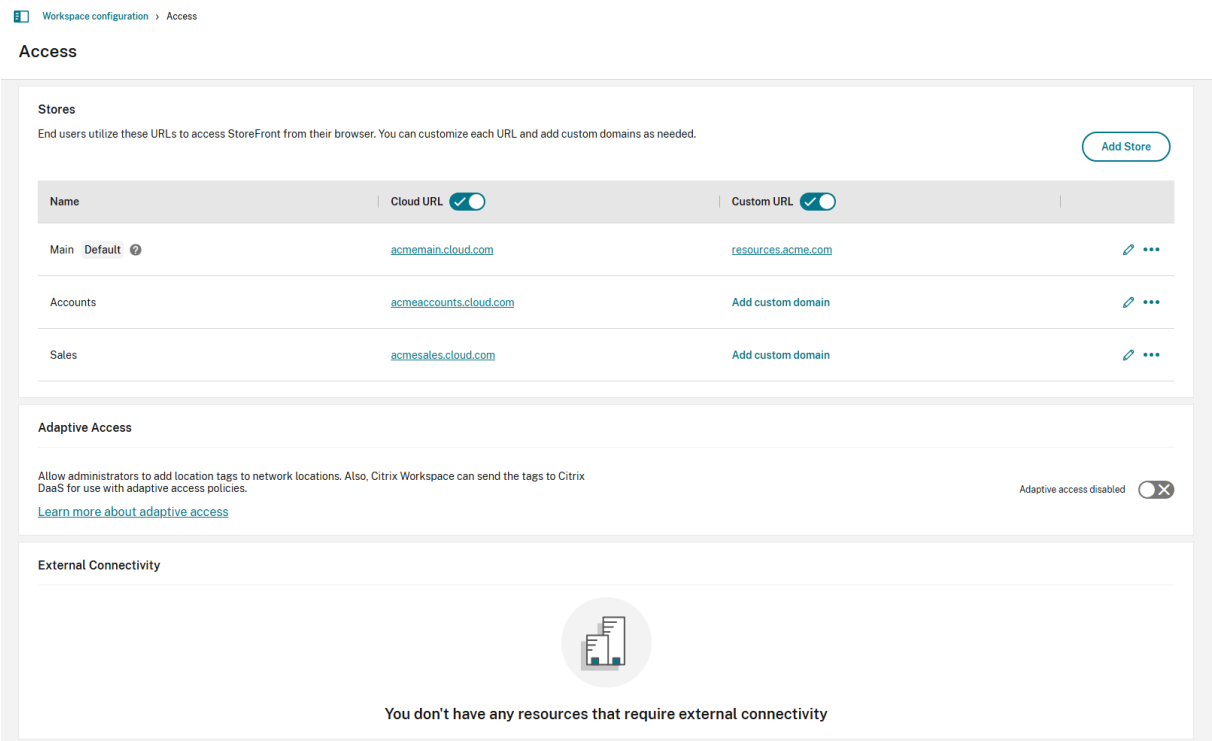
1. Go to the **Access** tab.
2. Go to the section **Adaptive access** and click the toggle. A confirmation screen appears.
3. Press **Disable**.

> **Warning:**
>
> The first time you enable **Adaptive access**, Citrix® StoreFront Cloud performs a one time migration of external connectivity configuration. Subsequently when you disable or enable Adaptive access then it switches between the configuration models which may impact user connections.
>
> Adaptive access affects how Delivery Group access policies are applied. When Adaptive access is enabled, connections appear as though they are via Access Gateway. When Adaptive access is disabled, connections appear as though they are not via Access Gateway. Therefore changing Adaptive access changes which access policy rules are applied, which may impact which resources your users can see.

### External connectivity

The **External connectivity** panel lists each resource location and allows you to configure how users connect to resources in those locations. For more information, see Connectivity to DaaS resources.




# Configure a custom domain

June 22, 2026

You can allow users to access their store using a custom domain instead or as well as the `cloud.com` domain. You must own the domain and each domain can only be used to access a single store.

Each cloud.com URL can have a linked custom URL.

## Prerequisites

- You can either choose a newly registered domain, or one that you already own. The domain must be in subdomain format (your.company.com). Citrix doesn't support using just a root domain (company.com).
- It recommended that you use a dedicated domain. This helps you change the domain easily, if necessary.
- Custom domains cannot contain any Citrix trademarks. Find the full list, see Cloud Software Group Trademark Guidelines.

- The domain you choose must be configured in the public DNS. Any CNAME record names and values included in your domain configuration must be resolvable by Citrix. Private DNS configurations are not supported.

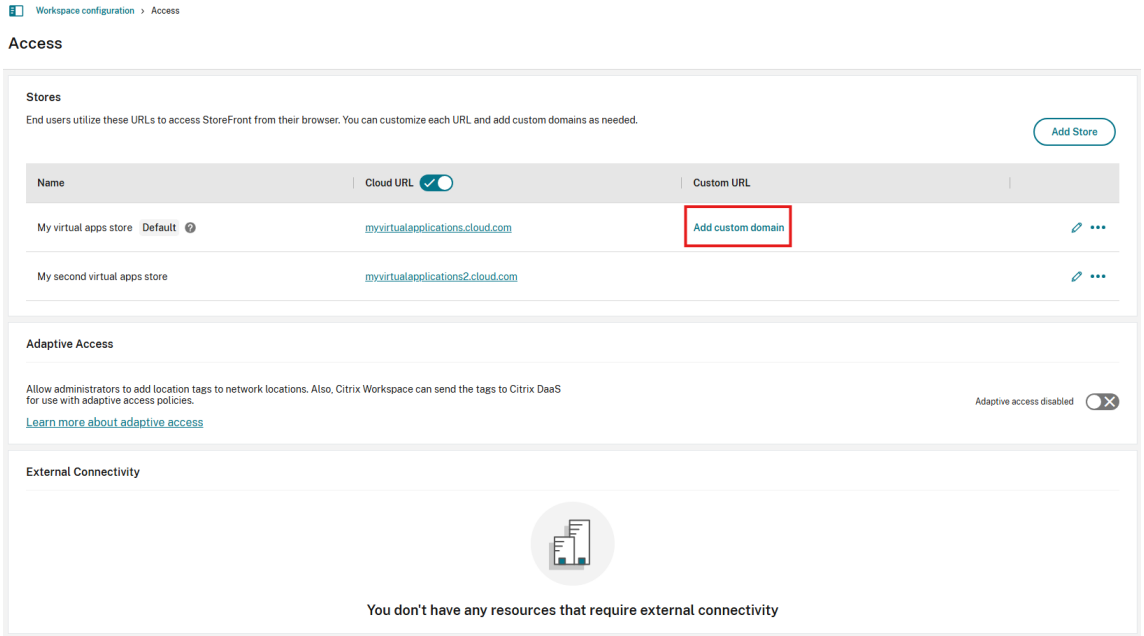
## Configuring your custom domain

Once a custom domain is set, you can't change the URL or certificate type. You can only delete it. Ensure that the domain you choose isn't already configured in DNS. Remove any existing **CNAME** records before attempting to configure your custom domain.

> **Note:**
>
> When adding the custom URL and configuring SAML, Citrix Cloud™ requires 24 hours for provisioning.

### Adding a custom domain

1. Sign in to Citrix Cloud.
2. From the Citrix Cloud menu, select **StoreFront Cloud** and then select **Access**.
3. On the **Access** tab, in the **Stores** table select **Add custom domain** for the cloud URL you want to add a custom URL for (the first custom URL you create must be associated with your primary cloud URL).




4. Read the information that appears on the **Overview** page, and select **Next**.

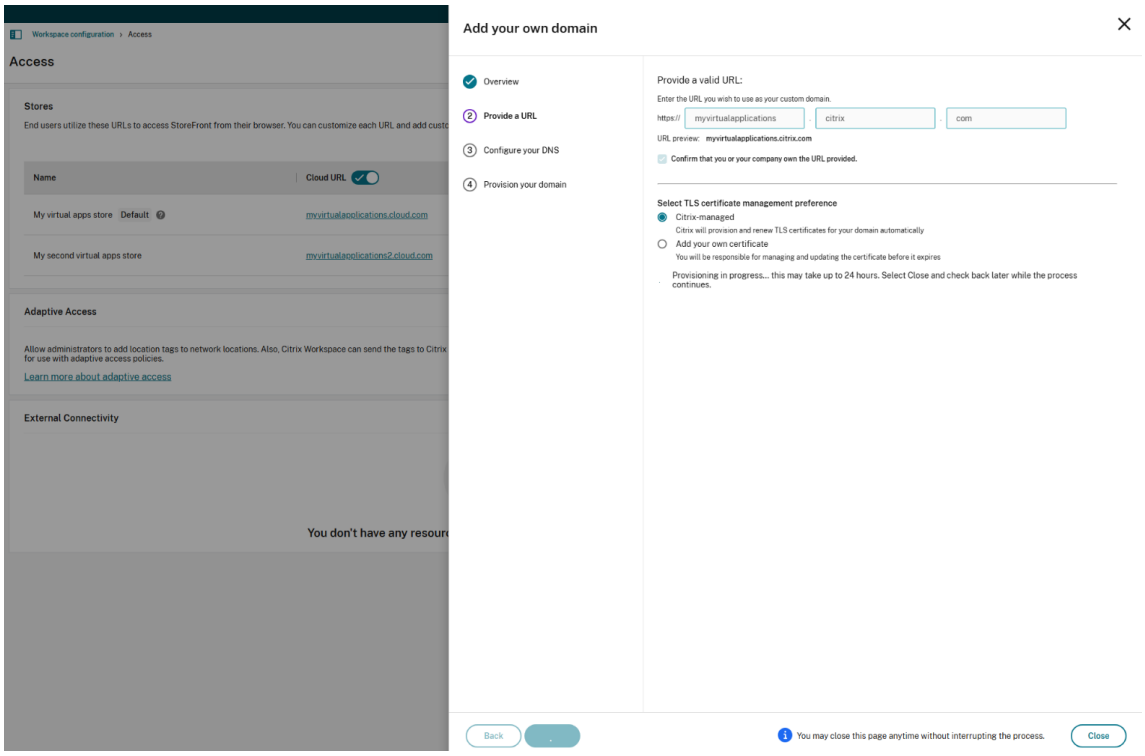
 

5. Enter your chosen domain in the **Provide a URL** page. Confirm that you own the specified domain by selecting **Confirm that you or your company own the URL provided**, and choose your TLS certificate management preference. It is recommended selecting **managed**, as the certificate renewals are handled for you. For more information, see Providing a renewed certificate. Click **Next**.

   If any warnings appear on this page, correct the highlighted issue to proceed.

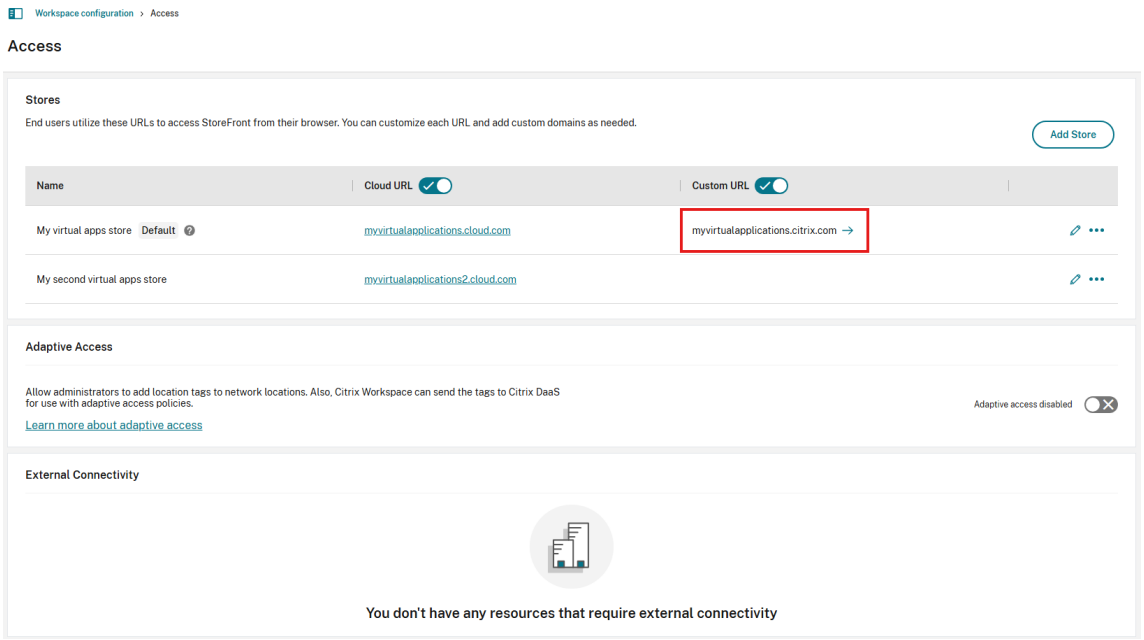
   If you have chosen to provide your own certificate, there's an extra step to complete in the instructions.

   Provisioning of your chosen domain takes some time. You can wait with the page open or close it while provisioning is in progress.




6. If you have the **Provide a URL** page open while provisioning completes, the **Configure your DNS** page opens automatically. If you have closed the page, select the **Continue** button for your custom domain from the **Access** tab.



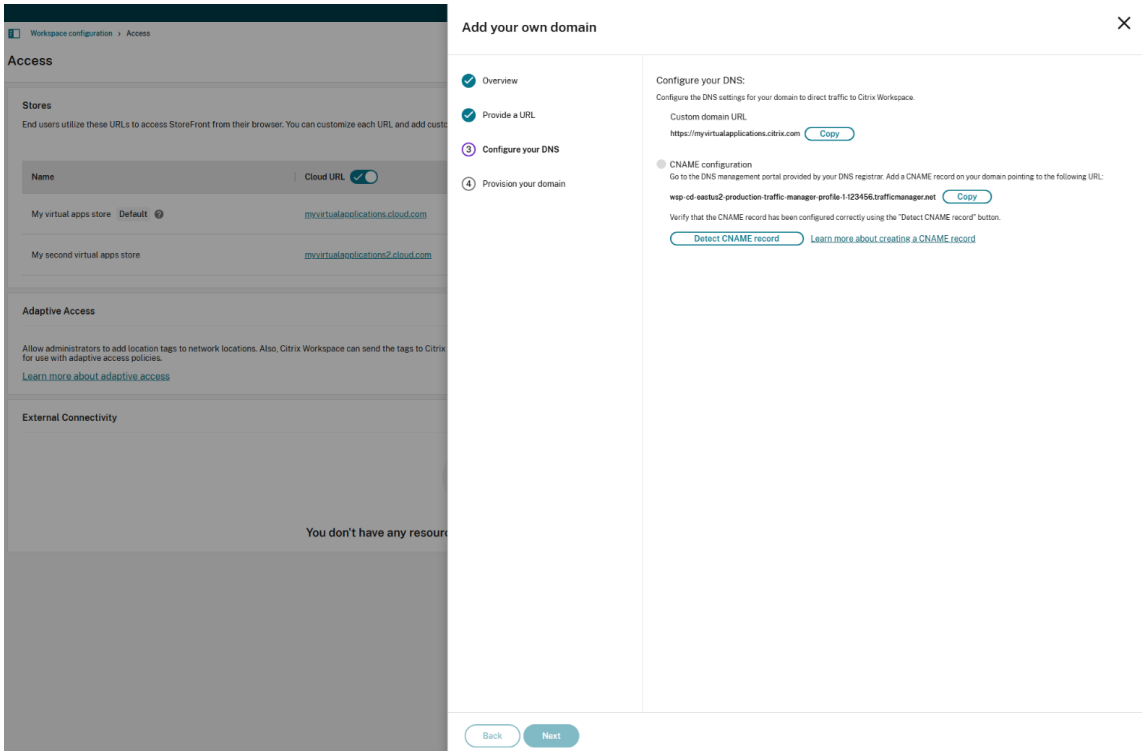

7. Perform this step in the management portal provided by your DNS registrar. Add a **CNAME** record for your chosen custom domain that points to the Azure Traffic Manager assigned to you.

   Copy the address of the traffic manager from the **Configure your DNS** page. The address in the example is as follows:

   *wsp-cd-eastus2-production-traffic-manager-profile-1-123456.trafficmanager.net*

   If you have any Certificate Authority Authorization (CAA) records configured in your DNS, add one that allows *Let's Encrypt* to generate certificates for your domain. *Let's Encrypt* is the Certificate Authority (CA) that Citrix uses to generate a certificate for your custom domain. The value for the CAA record must be as follows: *0 issue "letsencrypt.org"*



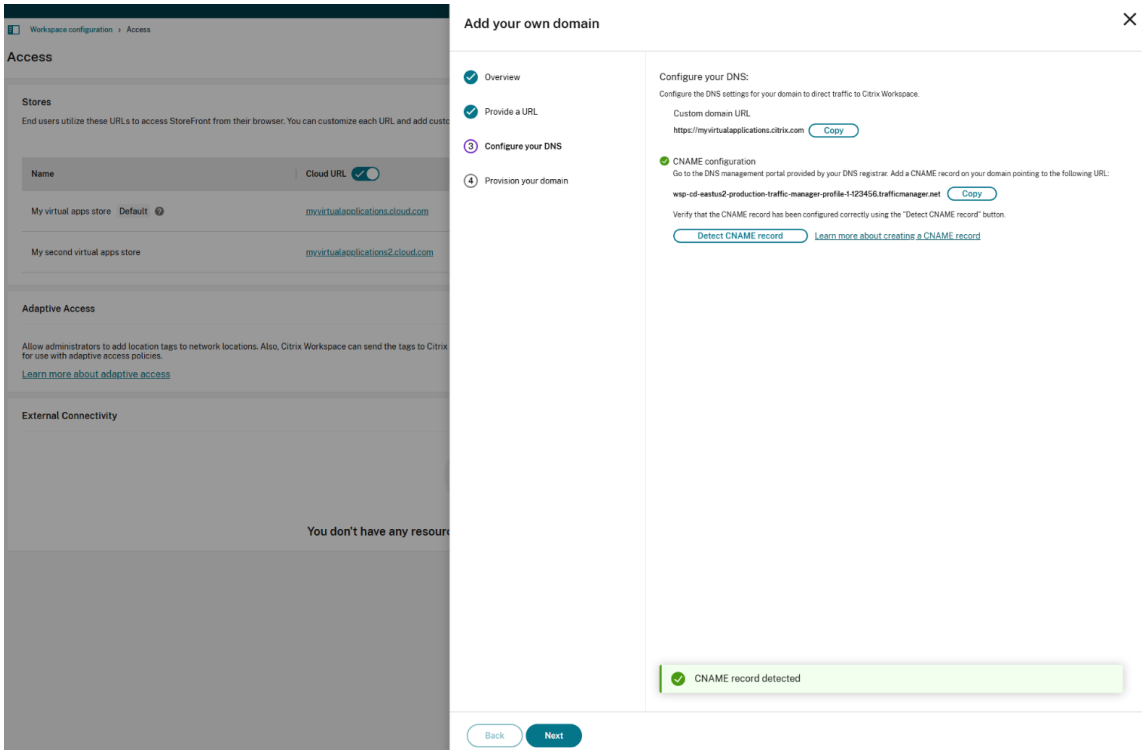

8. Once you configure the CNAME record with your DNS provider, select **Detect CNAME record** to verify that your DNS configuration is correct. If the CNAME record has been configured correctly, a green tick appears next to the **CNAME configuration** section.

   If any warnings appear on this page, correct the highlighted issue to continue.

   If you have any CAA records configured with your DNS provider a separate **CAA configuration** appears. Select **Detect CAA record** to verify that your DNS configuration is correct. If your CAA record configuration is correct, a green tick appears next to the **CAA configuration** section.

   When your DNS configuration is verified, click **Next**.



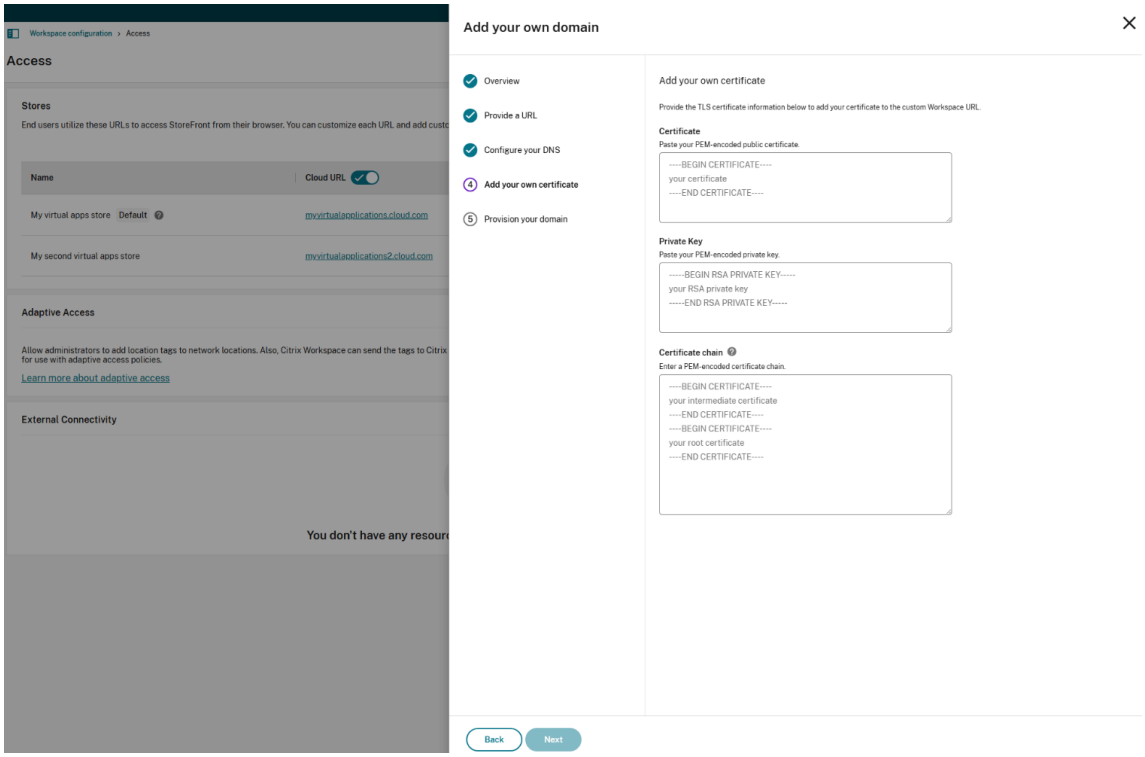

9. **This is an optional step**. If you chose to add your own certificate, complete the required information on the **Add your own certificate** page.

   > **Note:**
   >
   > Password protected certificates are not supported.

   If any warnings appear on this page, correct the highlighted issue to proceed.
   Ensure that the certificate fulfills the following conditions.

   - It must be PEM encoded.
   - It must remain valid for at least the next 30 days.
   - It must be used exclusively for the custom store URL. Wildcard certificates are not acceptable.
   - The common name of the certificate must match the custom domain.
   - SANs on the certificate must be for the custom domain. Additional SANs are not allowed.
   - The duration for which the certificate is valid must not exceed 10 years.

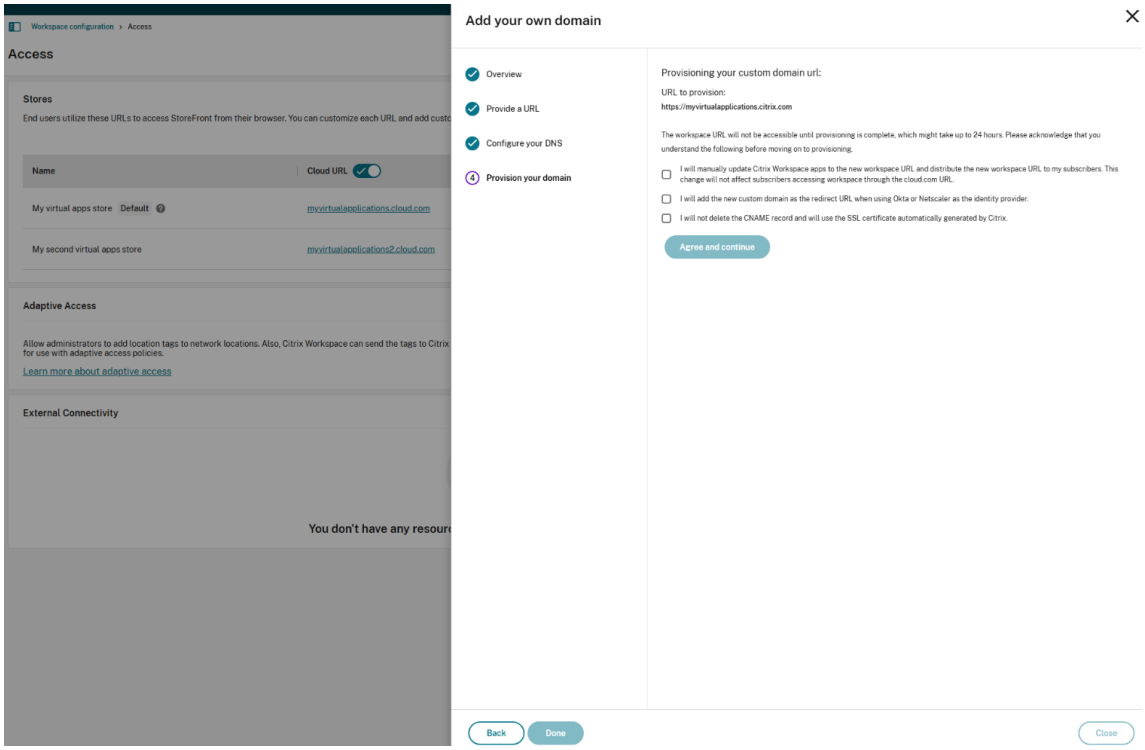



> **Note:**
>
> It is recommended that you use a certificate using a secure cryptographic hash function (SHA-256 or higher). You are responsible for renewing the certificate. If your certificate has expired or is about to expire, see the Providing a renewed certificate section.

10. Read the information that appears on the **Provision your domain** page and acknowledge the given instructions. When you're ready to continue, select **Agree and continue**.

    This final provisioning step can take some time to complete. You can wait with the page open while the operation completes, or you can close the page.




### Deleting a custom domain

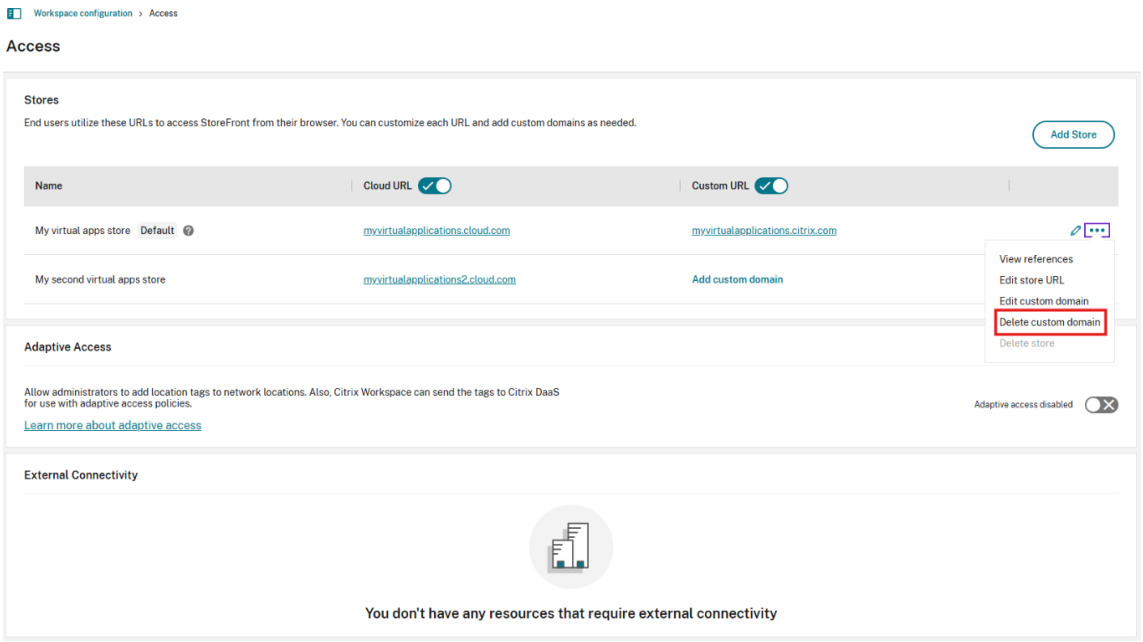
After deleting the custom URL, end users can only access the store using the cloud.com URL.

When you delete a custom domain, ensure that the CNAME record is removed from your DNS provider.

To delete a custom domain,

1. Sign in to Citrix Cloud.
2. From the Citrix Cloud menu, select **StoreFront Cloud > Access**.
3. Expand the context menu **(...)** for the custom domain on the **Access** tab, and select **Delete custom domain**.

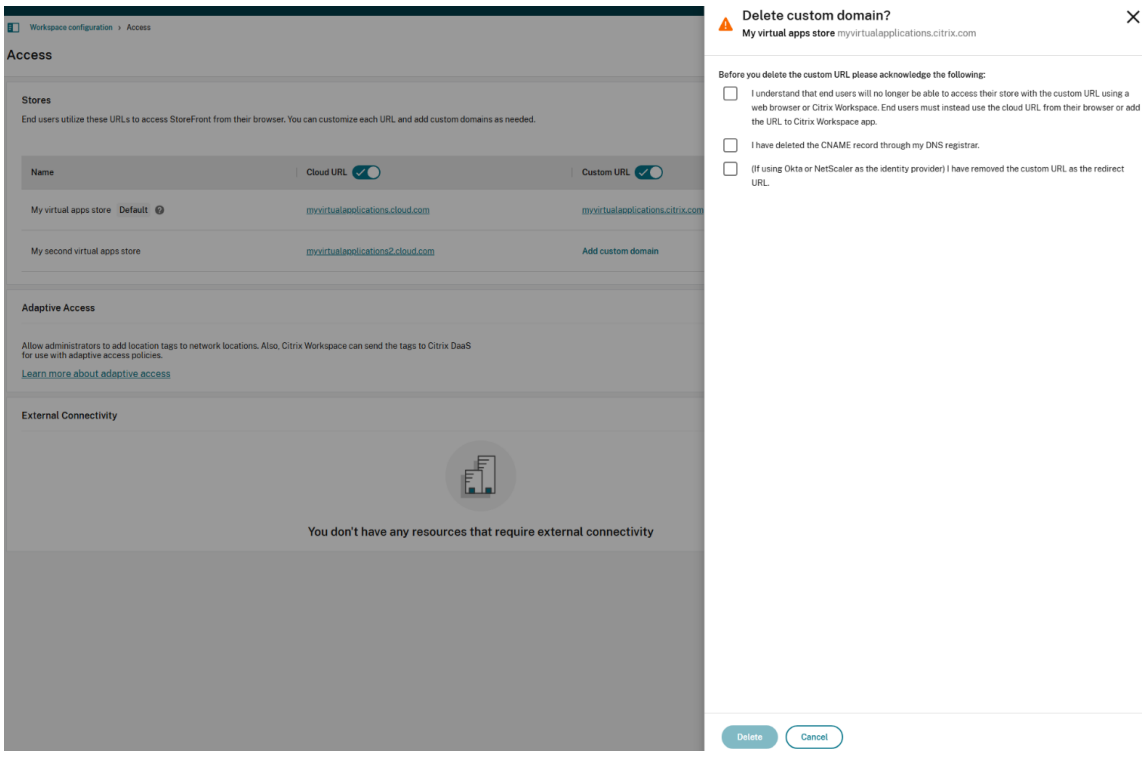
 




4. Read the information that appears on the **Delete custom domain** page and acknowledge the given instructions. When you're ready to continue, select **Delete**.

   Deleting a custom domain takes some time to complete. You can wait with the page open while the operation completes, or you can close the page.

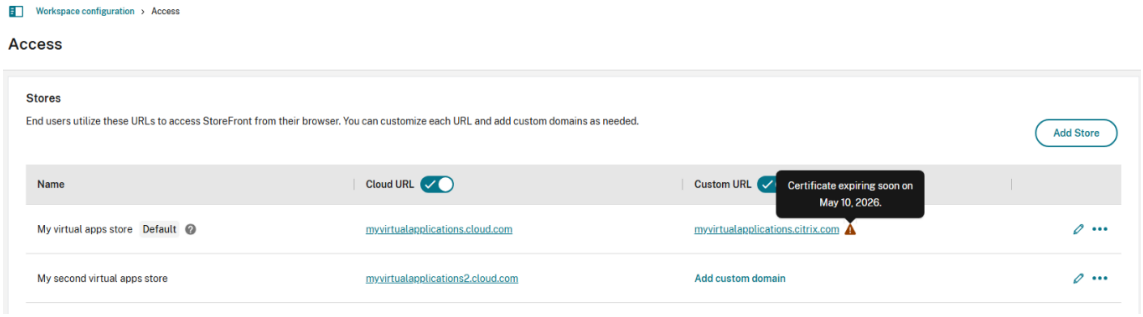
   If you have onboarded multiple custom domains, you cannot delete the custom domain associated with the default cloud URL until all other custom domains have been deleted.



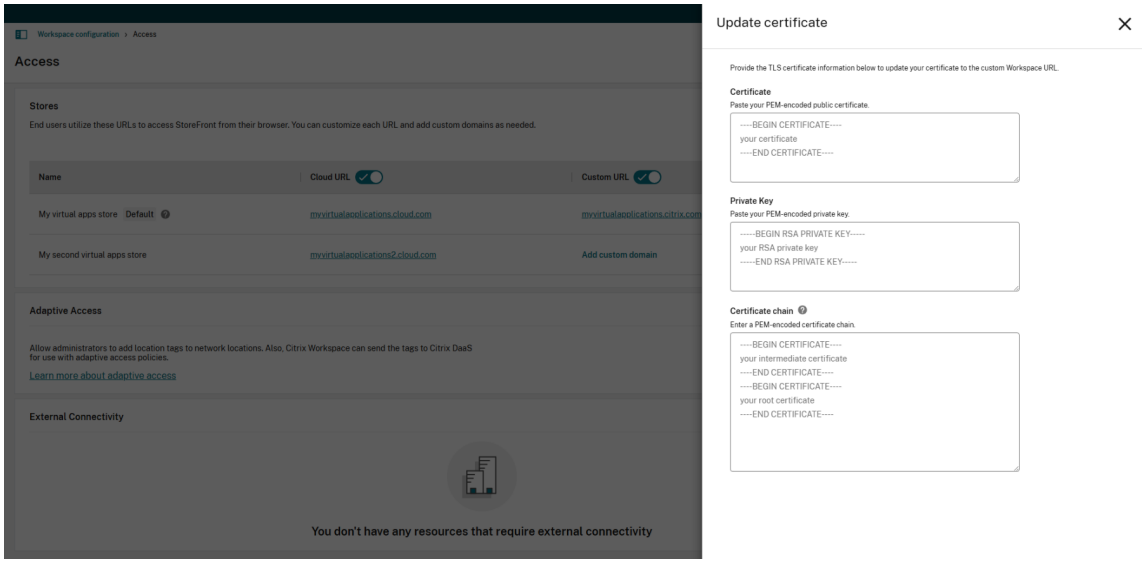

 

### Providing a renewed certificate

1. Sign in to Citrix Cloud.
2. From the Citrix Cloud menu, select **StoreFront Cloud** > **Access**.
3. When your certificate is about to expire in 30 days or less, your custom domain displays a warning.




4. Click the warning to open the update certificate wizard.




5. Enter the required information on the **Update certificate page**, and **Save**.

If any warnings appear on this page, correct the highlighted issue to proceed.

The certificate must meet the same requirements as when the custom domain was created. For more information, see Adding a custom domain.

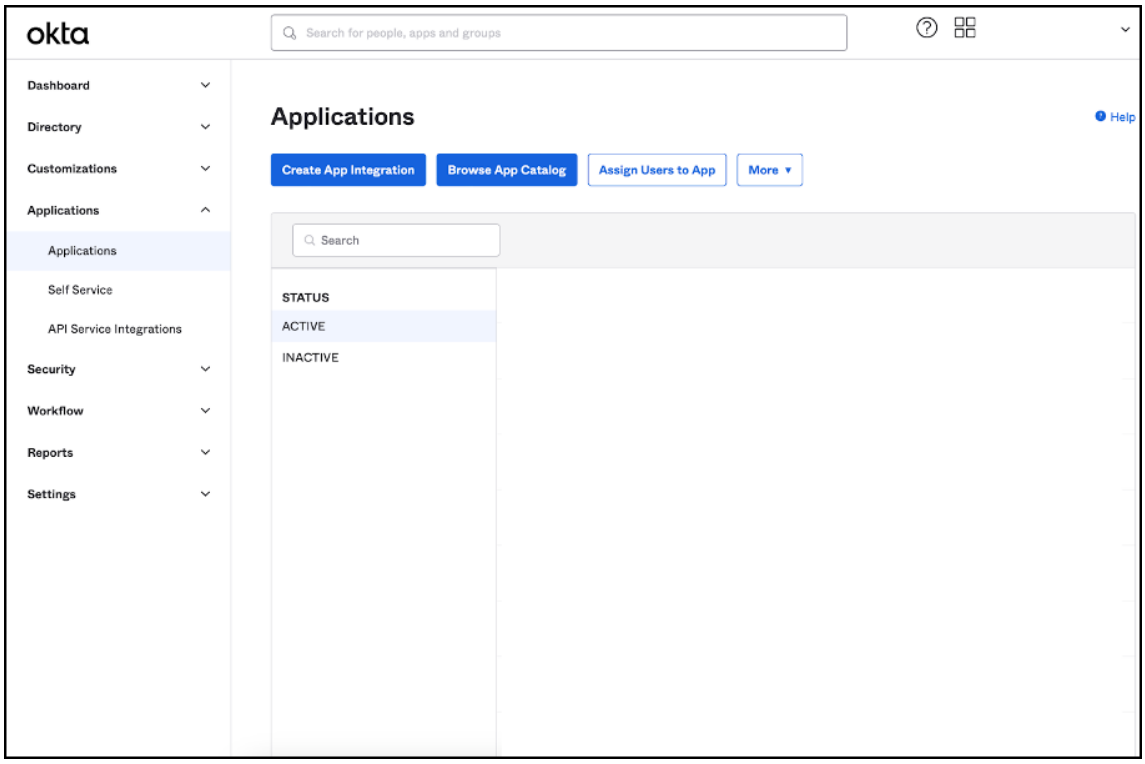
## Configuring your identity provider

### Configuring Okta

Perform the following steps if you are using Okta as the identity provider for store access.

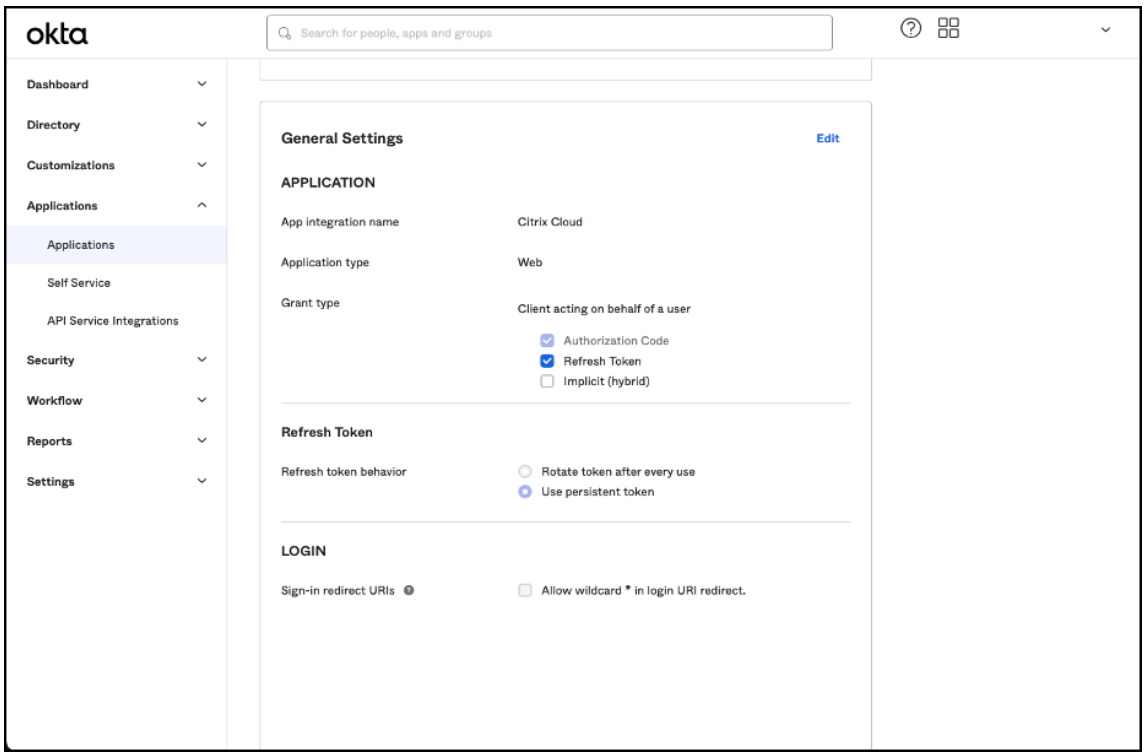
 

1. Sign in to the administrator portal for your Okta instance. This instance contains the application that is used by Citrix Cloud.
2. Expand **Applications** then select **Applications** in the menu.

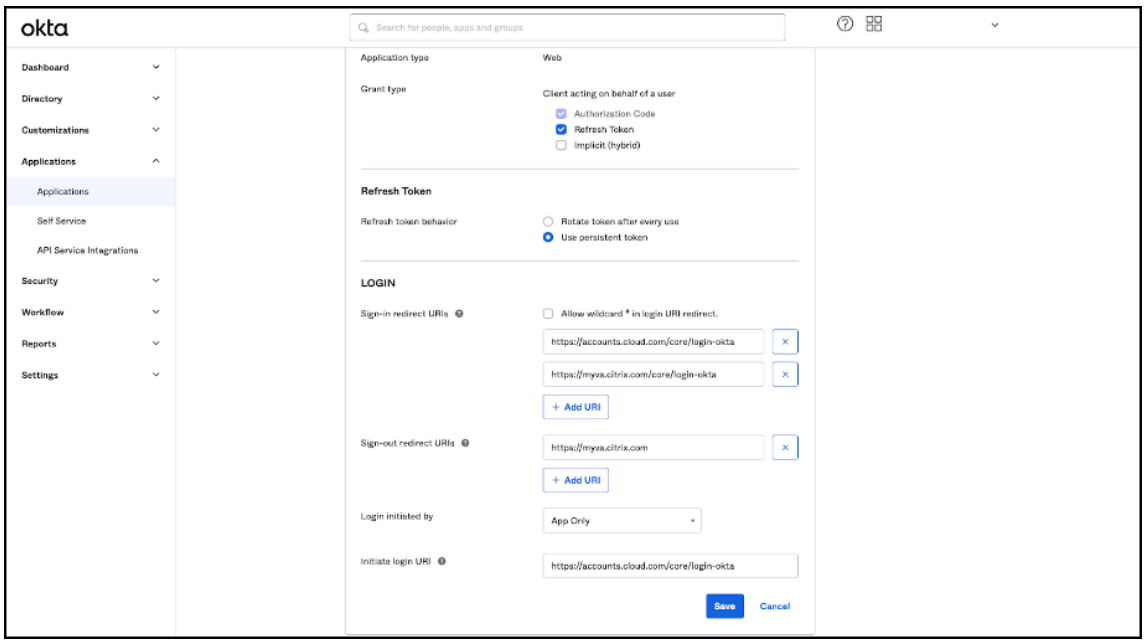



3. Open the application linked to Citrix Cloud.
4. Select **Edit** in the **General Settings** section.




5. In the **LOGIN** section of **General Settings**, add a value for **Sign-in redirect URIs**. Add the new value without replacing any existing values. The new value must be of the following format: `<https://your.company.com/core/login-okta>`
6. In the same section add another value for **Sign-out redirect URIs**. Add the new value without replacing any existing values. The new value must be in the following format: `<https://your.company.com>`



7. Click **Save** to store the new configuration.

> **Note:**
>
> To configure SAML with your custom domain, follow the procedure mentioned in SAML configuration.

## Configuring OAuth Policies and Profiles

> **Important**
>
> The existing OAuth policy and profile that links Citrix Cloud and Citrix Gateway or your Adaptive Authentication HA pair together, must be updated only if the OAuth credentials are lost. Altering this policy risks breaking the link between Citrix Cloud and stores and affects your ability to log in to stores.

### Configuring Citrix Gateway

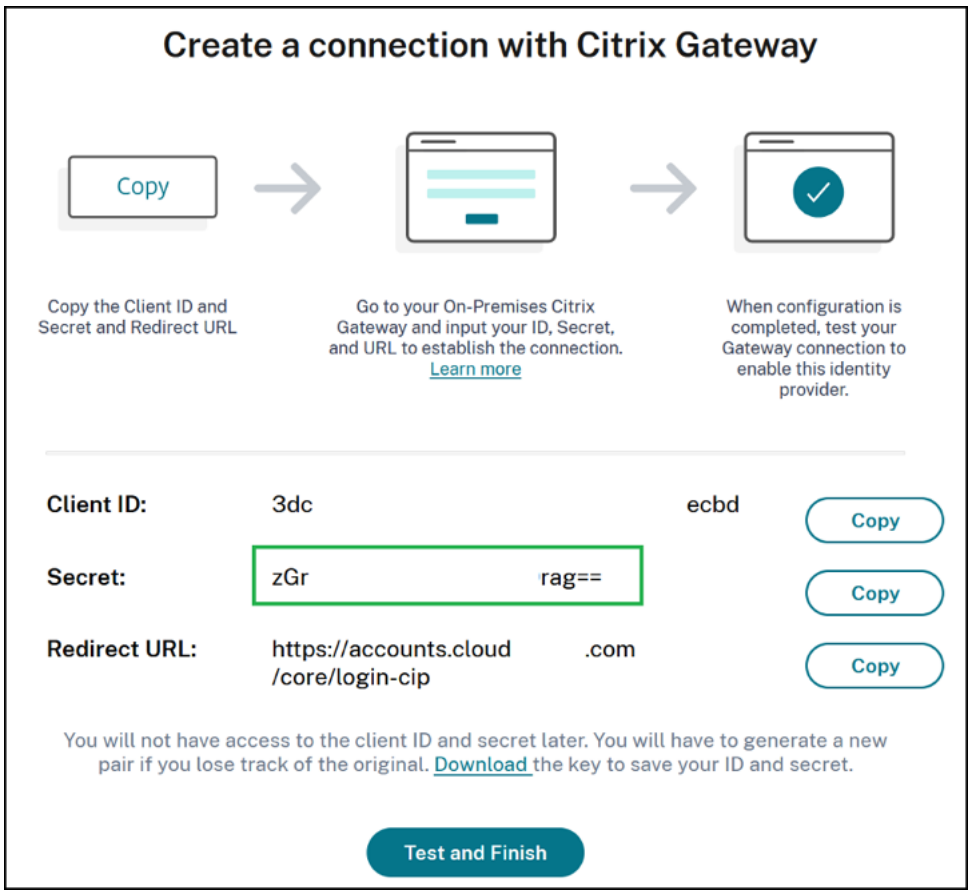
The Citrix Cloud admin has the access to the unencrypted client secret. These credentials are provided by Citrix Cloud during the Citrix Gateway linking process within **Identity and Access Management > Authentication**. The OAuth profile and policy is created by the Citrix admin. It is created manually on Citrix Gateway during the connection process.

You need the client ID and unencrypted client secret that were provided during the Citrix Gateway connection process. These credentials are provided by Citrix Cloud and have been saved securely. The unencrypted secret is needed to use both the Citrix ADC interface or the command-line interface (CLI) to create a OAuth policy and profile.

Here's an example of the UI when the client ID and secret are provided to the Citrix Admin.

> **Note:**
>
> The admin cannot obtain a copy of the unencrypted secret after the Citrix Gateway has been connected. They must save the credentials during the connection process.

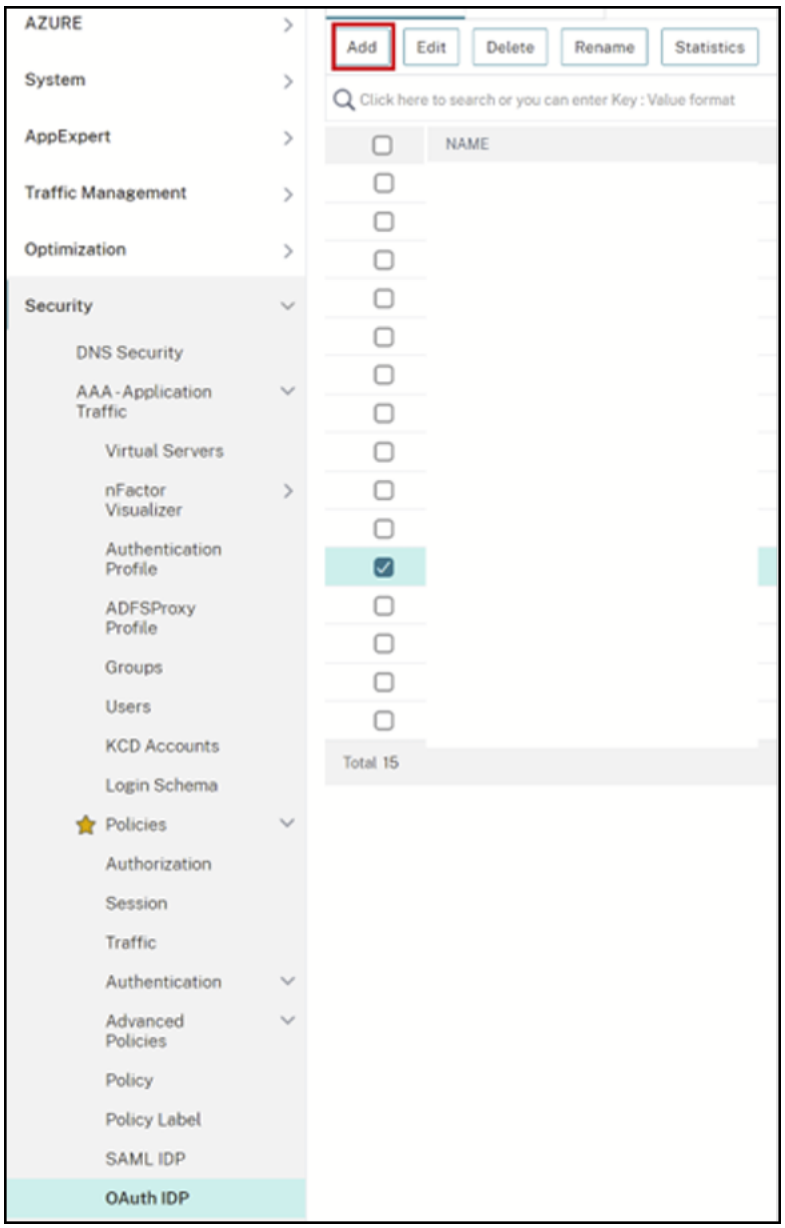
 




**Using Citrix Cloud** Perform these steps to add another OAuth profile and policy using the Citrix Gateway interface:

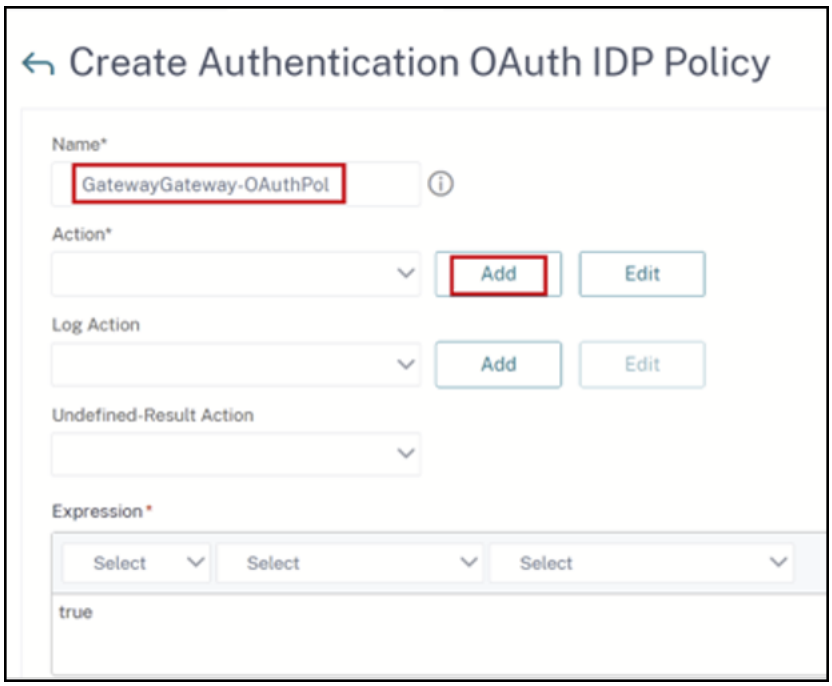
1. From the menu select **Security > AAA - Application Traffic > OAuth IDP**. Select the existing OAuth policy and click **Add**.



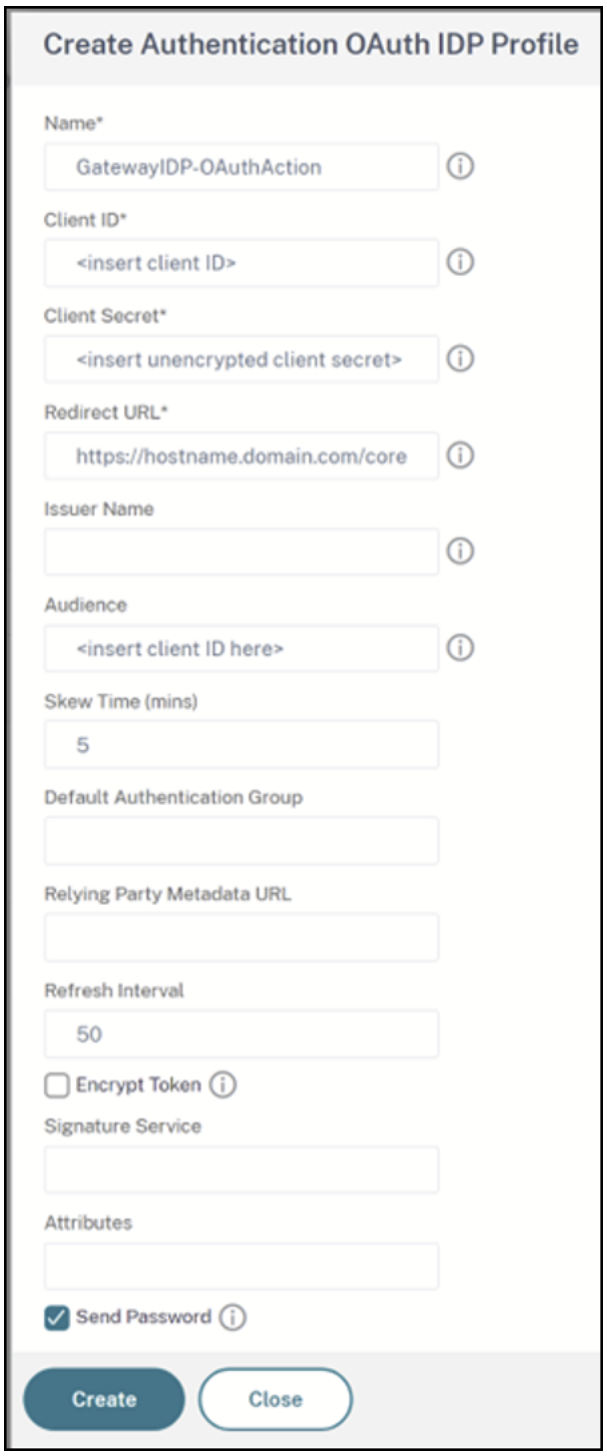

2. When prompted, modify the name of the new OAuth policy to be different from the existing policy selected the previous step. Citrix suggests adding a *custom-URL* to its name.




3. On the Citrix Gateway GUI, create your existing OAuth Profile
4. On the same GUI menu click **Add**.




5. On the Citrix Gateway GUI, bind the new OAuth Policy to your existing authentication, authorization, and auditing virtual server.
6. Navigate to **Security > Virtual Servers > Edit**.


### Using the command-line interface (CLI)

> **Important**
>
> If you don't have a copy of the OAuth credentials saved securely, you need to disconnect and reconnect your Citrix Gateway. Update your existing OAuth profile with new OAuth credentials provided by Citrix Cloud Identity and Access Management. This procedure is not recommended and must be used only if the old credentials are unrecoverable.

1. Use an SSH tool such as PuTTY to connect to your Citrix Gateway instance.
2. Create the OAuthProfile and OAuthPolicy. Add authentication OAuthIDPProfile.

   ```
   "CustomDomain-OAuthProfile"-clientID "<clientID>"-clientSecret "<unencrypted client secret>"-redirectURL "https://hostname.domain.com/core/login-cip"-audience "<clientID>"-sendPassword ON

   add authentication OAuthIDPPolicy "CustomDomain-OAuthPol"-rule true -action "CustomDomain-OAuthProfile"
   ```

3. Bind the OAuthPolicy to the correct authentication, authorization, and auditing virtual server with a lower priority than the existing policy. This instance assumes that the existing policy has a priority of 10, so 20 is used for the new policy. Bind authentication virtual server.

   ```
   "CitrixGatewayAAAvServer"-policy "CustomDomain-OAuthPol"-priority 20
   ```

### Configuring Adaptive Authentication

> **Important**
>
> The encrypted secret and encryption parameters for the OAuth profile are different on the Adaptive Authentication primary vs secondary HA gateways. Make sure you obtain the encrypted secret from the primary HA gateway and also run these commands on the primary HA gateway.

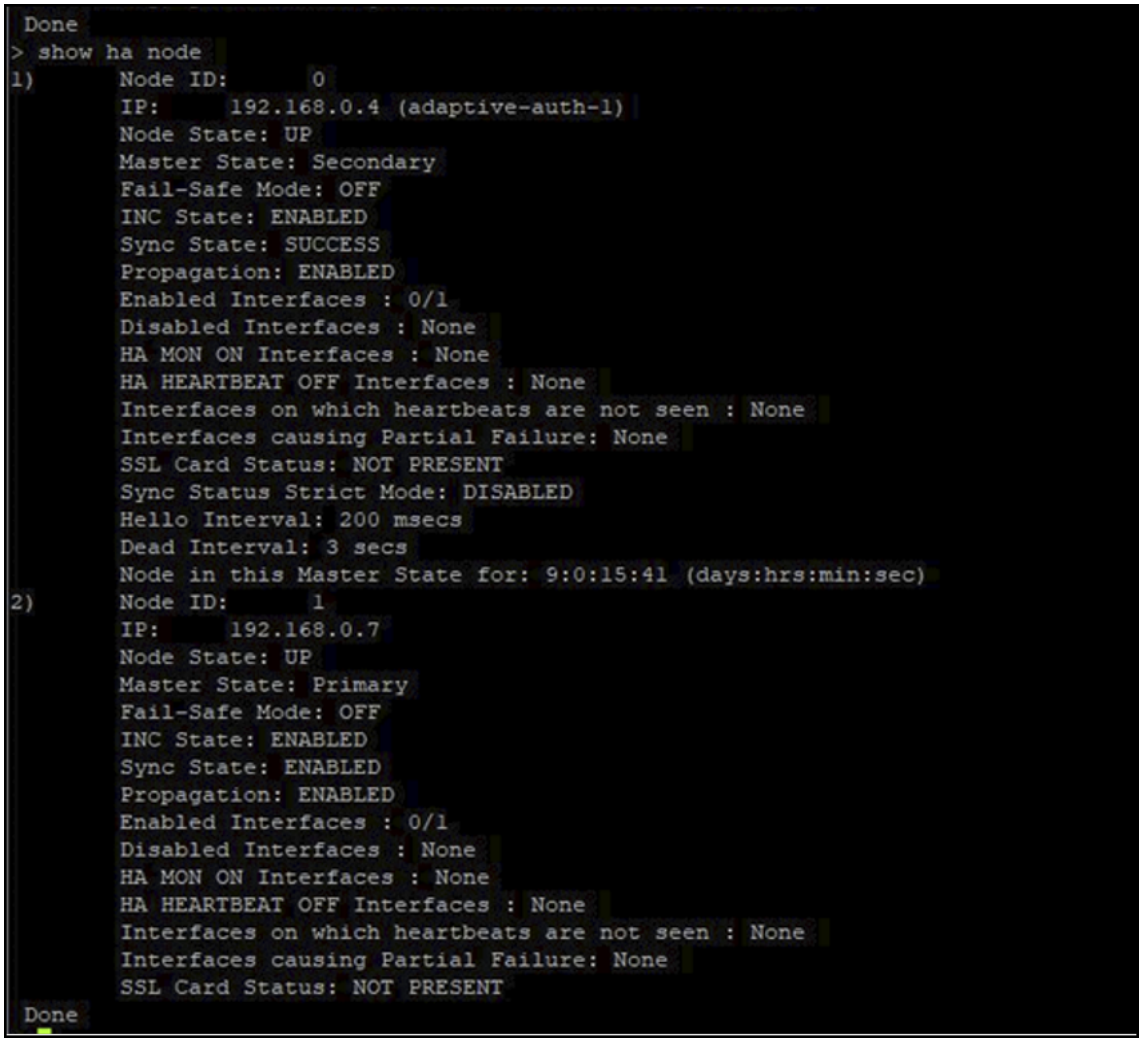
The Citrix Cloud admin doesn't have access to the unencrypted client secret. The OAuth policy and profile is created by the Citrix Adaptive auth service during the provisioning phase. It is necessary to use the encrypted secret and CLI commands obtained from the ns.conf file to create OAuth profiles. This cannot be performed using the Citrix ADC UI. Bind the new Custom URL OAuthPolicy to your existing authentication, authorization, and auditing virtual server using a higher priority number than the existing policy that is bound to your existing authentication, authorization, and auditing virtual

server. The lower priority numbers are evaluated first. Set the existing policy to be priority 10 and the new policy to be priority 20 to ensure they are evaluated in the correct order.

1. Connect to your Adaptive Authentication primary node using an SSH tool like PuTTY.

   ```
   show ha node
   ```

2. Locate the line within the running configuration of the primary HA gateway containing your existing OAuth Profile.

   ```
   sh runn | grep oauth
   ```

3. Copy the output from the Citrix ADC CLI including all encryption parameters.

4. Modify the line that you copied from the previous step. Use it to construct a new CLI command that allows you to create an OAuth profile using the encrypted version of the client ID. All encryption parameters must be included.

- Update the name of the OAuth profile to *CustomDomain-OAuthProfile*
- Update the -redirectURL to https://hostname.domain.com/core/login-cip

Following example covers both updates.

```
add authentication OAuthIDPProfile "CustomDomain-OAuthProfile"-
clientID b1656835-20d1-4f6b-addd-1a531fd253f6 -clientSecret <long
 encrypted client Secret> -encrypted -encryptmethod ENCMTHD_3
-kek -suffix 2023_04_19_09_12_25 -redirectURL "https://hostname
.domain.com/core/login-cip"-audience b1656835-20d1-4f6b-addd-1
a531fd253f6 -sendPassword ON

add authentication OAuthIDPPolicy "CustomDomain-OAuthPol"-rule
true -action "CustomDomain-OAuthProfile"
```

5. Bind the OAuthPolicy to the correct authentication, authorization, and auditing virtual server with a lower priority than the existing policy. The authentication, authorization, and auditing virtual server name for all Adaptive Authentication deployments is the name *auth_vs*. This instance assumes that the existing policy has a priority of 10, so 20 is used for the new policy.

   ```
   bind authentication vserver "auth_vs"-policy "CustomDomain-
   OAuthPol"-priority 20
   ```

### Known limitations

Some known limitations of the custom domain solution are as follows:

- The first custom domain you create must be linked to the default cloud URL. Custom domains can then be added to other cloud URLs added through the multi-URL feature after a custom domain has been created for the default cloud URL.
- If you have onboarded multiple custom domains, you cannot delete the custom domain associated with the default cloud URL until all other custom domains have been deleted.
- This feature is not supported on Citrix Workspace app for Windows version 2305 and 2307. Update to the latest supported version.
- Logging on using a custom domain with Google authentication isn't supported.

## Configure store URLs

June 22, 2026

### Overview

When you first enable store, the system creates a store URL of the form `customername.cloud.com` that can be used to access the store from web browsers or locally installed Citrix Workspace™ app.

You can add additional cloud URLs. If you have defined multiple store URLs, you can use these URLs as policy inputs. For example, you might want different branding, authentication methods, and resources for different divisions within your organization.

You can also use your own custom domains linked as aliases for your cloud.com domains. For more information, see configure custom domain.

### Store name

Each store URL has a Store name. This name is displayed in the Accounts list within Citrix Workspace app.

You configure whether the user can modify the store name within Citrix Workspace app. To allow users to edit their store name from the Citrix Workspace app, users must be on the following versions of the Citrix Workspace app clients:

- Citrix Workspace app for Windows version 2405 or later
- Citrix Workspace app for iOS version 24.2.0 or later
- Citrix Workspace app for Mac version 2402

### Enable or disable cloud URL

You can disable all access to your stores using cloud URLs. This affects both locally installed Citrix Workspace app and browsers. Users can continue to use any custom URLs to access their stores. If you do not have any custom URLs then this blocks all access.

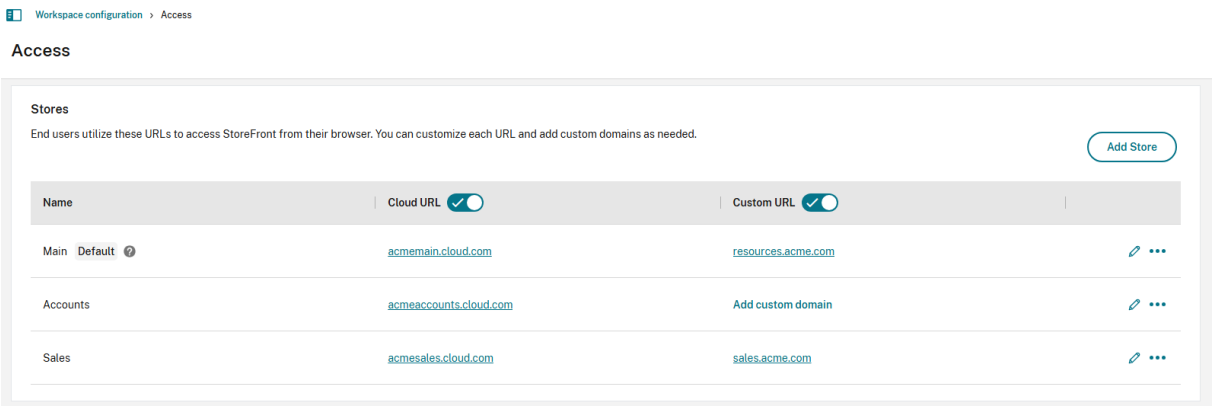
To disable access via cloud.com:

1. Untick the **Cloud URL** radio button. This brings up a confirmation screen.
2. Select the checkboxes to confirm you understand.
3. Press **Disable**.

### View URLs

1. Go to Citrix Cloud™ and sign in with your credentials.
2. Navigate to **StoreFront Cloud** > **Access**. Under **Stores**, you can find a list of existing URLs.




## Add store (Cloud) URLs

Select a unique store URL. Citrix Cloud rejects store URLs that other customers already use. Use a naming convention that contains a string unique to your organization. Avoid generic URLs such as `store.cloud.com` or `mystore.cloud.com`.

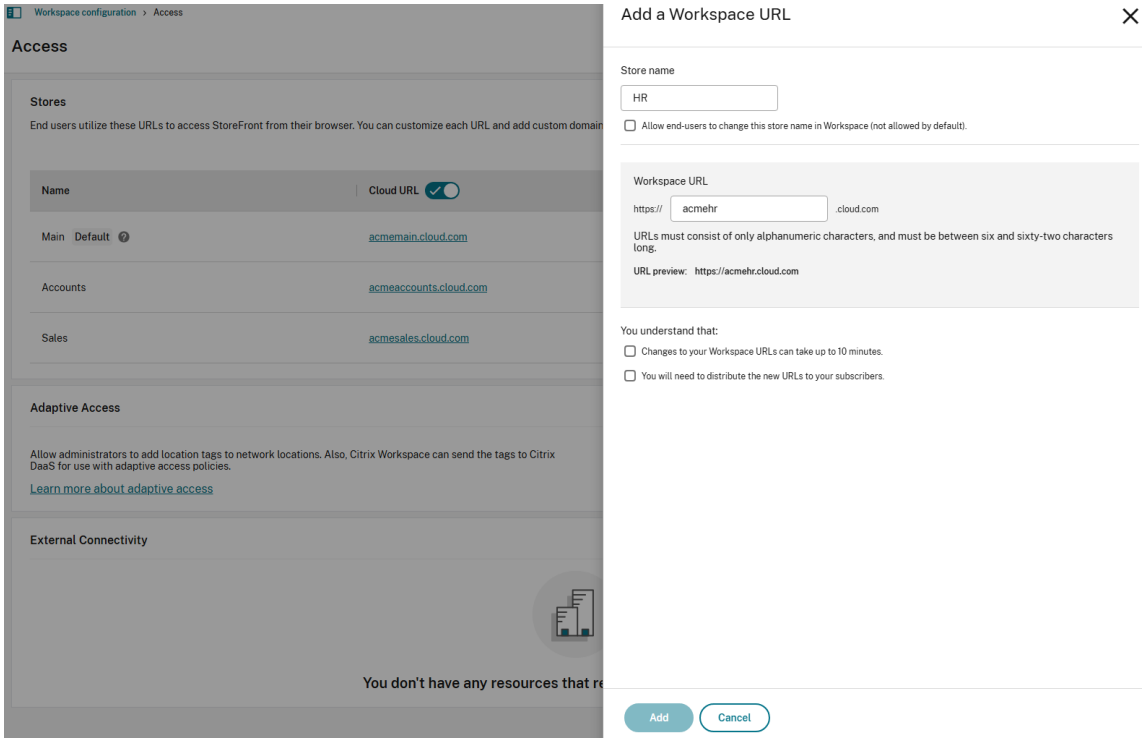
For example, you can create URLs using the following format:

- `YourOrgsales.cloud.com`
- `YourOrgengineering.cloud.com`
- `YourOrgmarketing.cloud.com`

From the Access tab, to add a URL:

1. Click **Add Store**
2. Enter a store name.
3. Choose whether you wish the user to be able to modify the store name within Citrix Workspace app.
4. Enter the subdomain.




5. Select the checkboxes as an acknowledgment that you must provide the new URLs to your end users post configuration.
6. Click **Add** to save the URL.

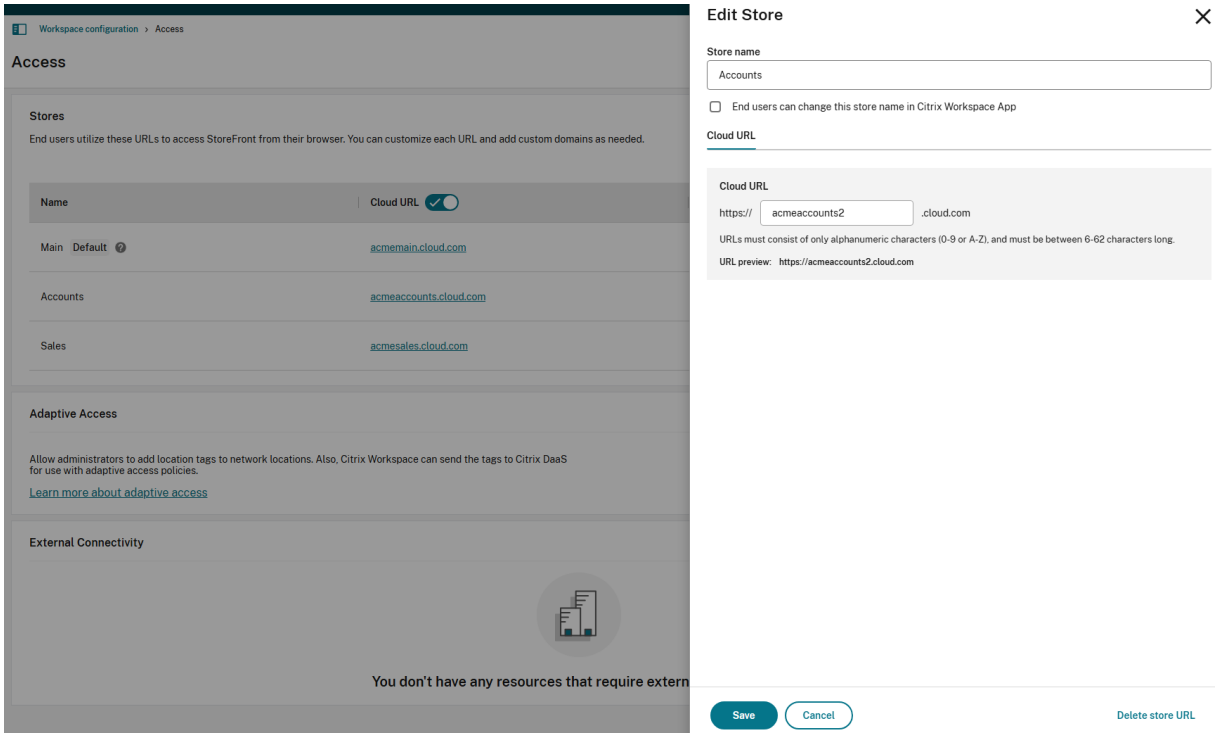
> **Note:**
>
> You can create up to 10 URLs by default. Contact your Citrix representative if you need more URLs.

## Modify store (Cloud) URL

> **Warning:**
>
> When you rename a URL, the old URL is immediately removed and is no longer available. Tell end users what the new URL is and manually update all local Citrix Workspace apps to use the new URL. The new URL will be unavailable for up to 10 minutes. If the URL is used in any policy then you must manually update that policy.

1. Click the **...** on the row of the store URL you wish to edit and select **Edit store URL**.
2. Modify the Store name and Cloud URL as required.
3. If you modified the URL then you must tick several checkboxes to acknowledge that you understand the consequences.




1. Press Edit to save the changes

### Configure store URLs using PowerShell

You can also use the PowerShell API to add or change store URLs.

Run the cmdlet `Set-WorkspaceCustomConfigurations` with the `$storeHosts` list as the argument to the `-WorkspaceHosts` parameter to update the URL list for the store. Give the existing URL as the argument to the `-WorkspaceUrl` parameter. For example:

```
#  Set a variable to the value of existing URL for the store.
$WSPURL = "wspmultiurlmain.cloud.com"

# Specify the new URLs that you want to create in a list, including any existing URLs.
$storeHosts = @($WSPURL,"wspmultiurl2.cloud.com","wspmultiurl3.cloud.com")

# Update the configuration
Set-WorkspaceCustomConfigurations -WorkspaceUrl $WSPURL `
                                  -WorkspaceHosts $storeHosts `
                                  -ClientId $APIClientID `
                                  -ClientSecret $APIClientSecret `
                                  -Verbose
```

```
Name                           Value
----                           -----
windowsShareIdpSessions
disallowICADownload            False
macShareIdpSessions
androidWebviewtype
iosWebviewtype
inactivityTimeoutInMinutesM...
linuxShareIdpSessions
idpdomains
inactivityTimeoutInMinutes
workspaceHosts                 {wspmultiurlmain.cloud.com, wspmultiurl2.cloud.com, wspmultiurl3.cloud.com}
```

### Configure authentication methods

To configure different authentication methods per URLs:

1. Create a conditional authentication profile.
2. Add a **Policy Condition** of type **Workspace URL** and select the store URL the condition should apply to.
3. Choose the authentication method for that store URL.
4. Repeat for each store URL.
5. In the Stores Authentication tab, choose the conditional authentication profile that you created.

Alternatively if you are using Adaptive Authentication, see Configure Adaptive Authentication policies.

### Configure themes and logos

You can create and assign separate themes and logos for each store. For more information, see Appearance.

### Resource filtering using Secure Private Access

While configuring Citrix DaaS™ with Secure Private Access, you can control the end user's access to resources. You can implement this by configuring Access policies based on store URLs. Access Policies can be configured for delivery groups using the store URL filter.

For more information, see Citrix Secure Private Access

### Send custom announcements

You can display a different custom announcement to your user depending on their store URL. For more information, see Send custom announcements.

### Resource Filtering resources from DaaS

You can configure Access Policies for delivery groups based on store URLs. For more information, see Resource filtering using delivery group access policies.

### Configure Adaptive Authentication policies

If you are using Adaptive Authentication, you can associate authentication policies with a store URL. This enables you to configure different authentication policies for the end users based on the store URL they're using.

**Step 1:** Configure a series of authentication actions and policies that you want to use for the store URLs. The policy configuration depends on the type of authentication and the authentication factors that you want to use. Any supported nFactor authentication flow can be used.

For more information, see Adaptive Authentication

For example, consider the following scenario where:

- The first URL <https://wspmultiurlmain.cloud.com> must be mapped to LDAP authentication and OTP.
- The second URL <https://wspmultiurl2.cloud.com> must be mapped to LDAP authentication.
- The third URL <https://wspmultiurl3.cloud.com> must have End User Cert authentication

Examples:

Check for a particular store URL using exact string matching.

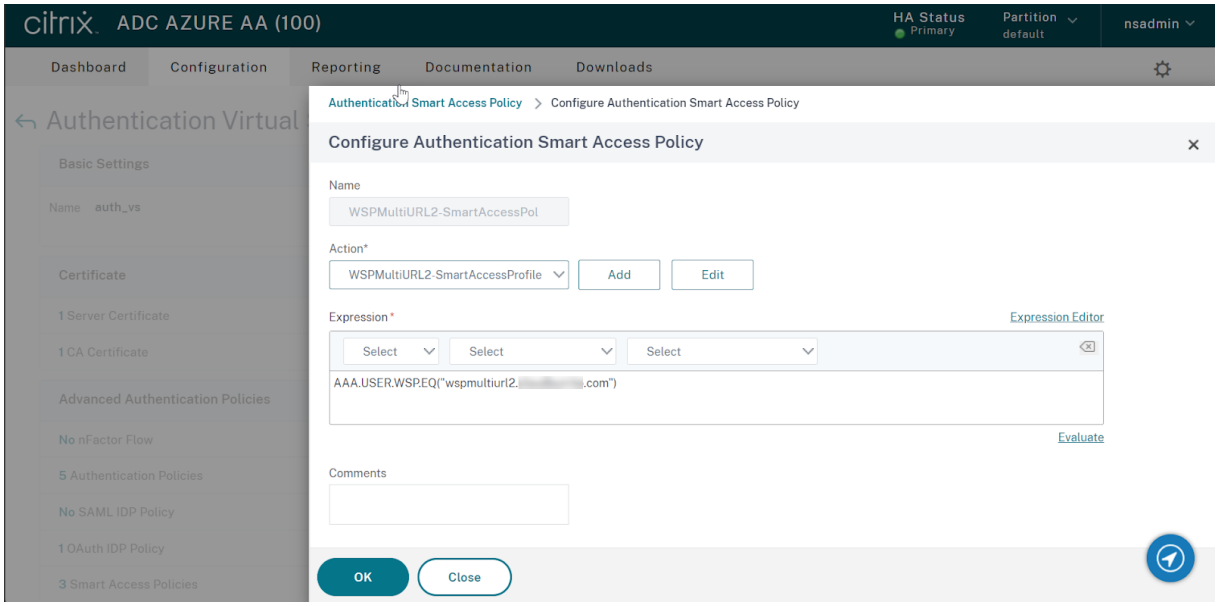
```
AAA.USER.WSP.EQ("wspmultiurlmain.cloud.com")
```

Check whether a particular string is contained within a store URL, using substring matching.

```
AAA.USER.WSP.CONTAINS("wspmultiurlmain")
```

**Step 2:** Configure an authentication policy and add your store URL as the expression. The authentication policy is then valid for the store URL that you entered in the **Expression** text field.




**Step 3:** Once you have configured authentication policies based on your URLs, you need to bind them to your authentication virtual server. For more information, see Authentication policies.

### Email Discovery to add store URLs to Citrix Workspace app

Email discovery adds all the store URLs configured in the list of service URLs as stores. If you want to add two or more stores through email discovery, configure each store URL as a service URL. It ensures that the URLs are added as stores during the email discovery process.
You can use either of the following methods to add stores:

- Global App Configuration service UI: For more info, see Configure settings for cloud store
- Global App Configuration API: You can use the preceding portal to make an API call to POST /aca/discovery/app/workspace/domain using your registered domain For more info, see Global App Configuration service API.

If <user@yourdomain.com> is entered in the Citrix Workspace app, the Email Discovery service adds all stores listed in service URLs. You can use a UPN, or an email address when it contains the correct domain suffix mydomain.com.

### Known limitations

The following are some limitations that impact the multiple URL feature.

**Citrix Virtual Apps and Desktops™**

- Resource filtering using store URL for Citrix Virtual Apps and Desktops (on-premises aggregation) isn't supported.

**Citrix Workspace app** To add multiple URLs from the same Citrix Cloud tenant to Citrix Workspace app requires the following versions:

- Citrix Workspace app for Windows version 2302 or later
- Citrix Workspace app for iOS version 2303 or later
- Citrix Workspace app for Android version 2303 or later
- Citrix Workspace app for Linux version 2303 or later
- Citrix Workspace app for Mac version 2305
- Citrix Workspace app for iOS version 2303
- Older versions of Citrix Workspace app display a store domain selector menu. In this case, the end user must select the same URL they entered when adding the store. Selecting a different URL requires the user to sign in again.

**Global App Configuration Service**

- If the Global App Configuration service settings are configured for multiple store URLs, then only one store URL can be added to Citrix Workspace app at a time. Adding a second URL to Citrix Workspace app fails. For example, If GACS settings are configured for both <https://wspmultiurlmain.yourdomain.com:443> and <https://wspmultiurl2.yourdomain.com:443> , then the user can add only one URL to Citrix Workspace app.
- Account addition fails if more than one GACS configured URL is found during the Global App Configuration service discovery. For example, consider a case where a user enters <user@yourdomain.com> in Citrix Workspace app. The domain-based discovery finds two results and GACS settings are configured for both of them. The response returned is: <https://wspmultiurlmain.yourdomain.com:443> and <https://wspmultiurl2.yourdomain.com:443>. In this case, account addition fails with Citrix Workspace app as it supports adding only one account with GACS settings configuration.

```
{

  "items": [
 {

   "domain": {

     "name": "yourdomain.com"
```

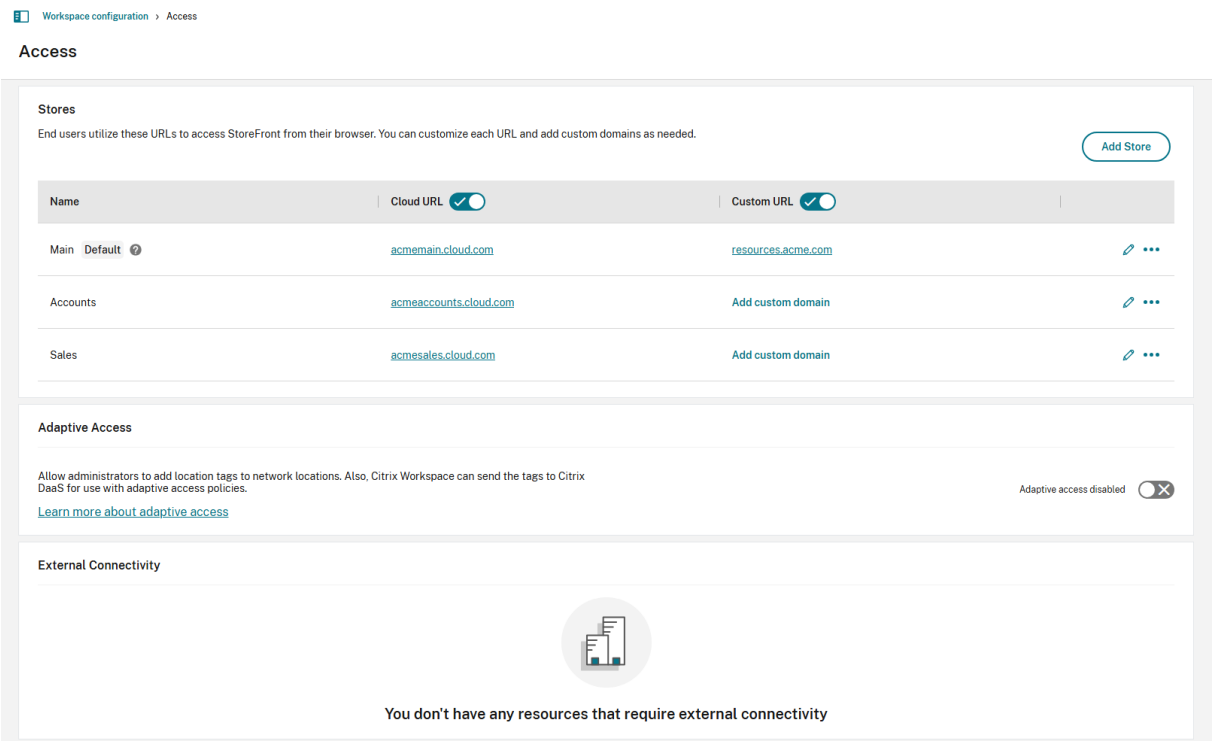
```
    }
,
  "app": {

    "workspace": {

      "serviceURLs": [
        {

          "url": "https://wspmultiurlmain.yourdomain.com:443"
        }
,
        {

          "url": "https://wspmultiurl2.yourdomain.com:443"
        }
,
        {

          "url": "https://wspmultiurl3.yourdomain.com:443"
        }

      ]
     }

   }

 }

 ],
 "nextToken": "None",
 "count": 1
}
```

## Connectivity to DaaS resources

June 22, 2026

Devices that are not on the same network as the VDAs hosting your virtual apps and desktops must connect via Citrix Gateway Service or a NetScaler Gateway. The **Exernal connectivity** panel lists each resource locations and allows you to configure how users connect to DaaS resources in those locations.




The experience depends on whether Adaptive access is enabled.

### Connectivity options when Adaptive access is disabled

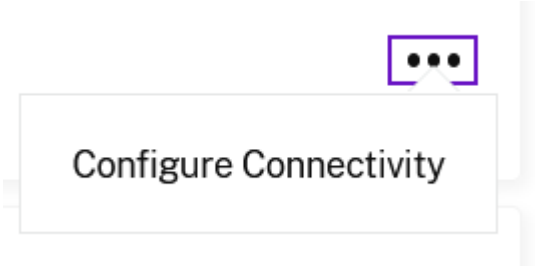
If Adaptive access is disabled then you can define a single Gateway for each resource location. The system uses this gateway unless:

- The device's public IP address matches a Network location. When Adaptive access is disabled, Network Locations do not have a connectivity type; all network locations are considered to be internal.
    - If your end users use a web browser to open apps and desktops, the client uses Websockets to connect to the VDA which requires the VDAs are configured for TLS. If the VDA does not have TLS enabled, Citrix® StoreFront Cloud always routes launches through a gateway, even for internal network locations.
    - When defining network locations, it is not possible to distinguish networks that share the same public IP address. For instance if your corporate network and guest wi-fi both use the same public IP address, and you create a Network location for this IP, this will prevent the gateway from being used for the guest wi-fi which may not be desired.
- HDX direct is enabled and the client determines that it can bypass the gateway and connect directly to the resource. When using HDX direct, there is no need to define network locations to allow direct connectivity.

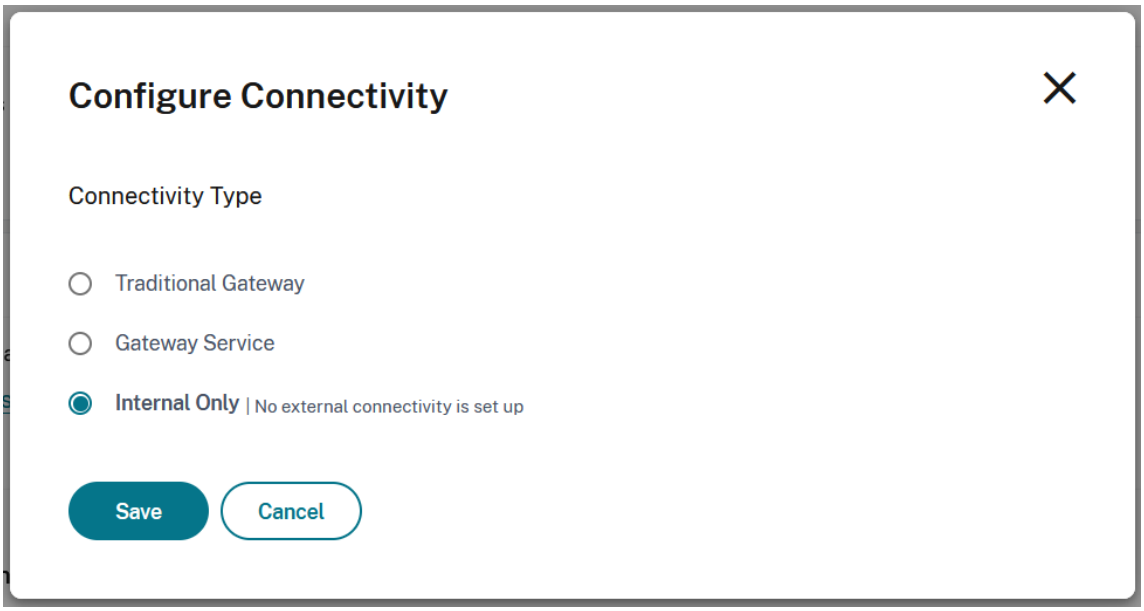
 

To edit the connectivity options:

1. Select ... to open the menu




2. Select **Configure Connectivity**.




3. Choose and configure the desired connectivity option.
   - Traditional Gateway
   - Gateway Service
   - Internal only
4. Select **Save**.

### Traditional Gateway

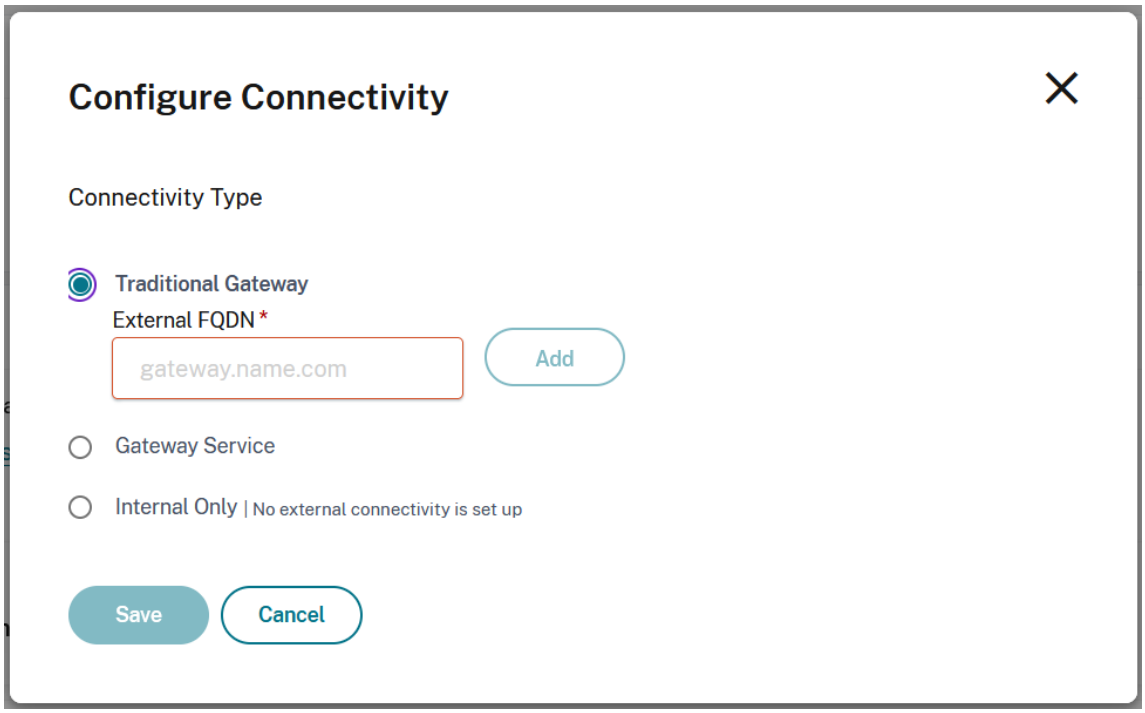
You can use a NetScaler gateway for HDX routing.

> **Warning**

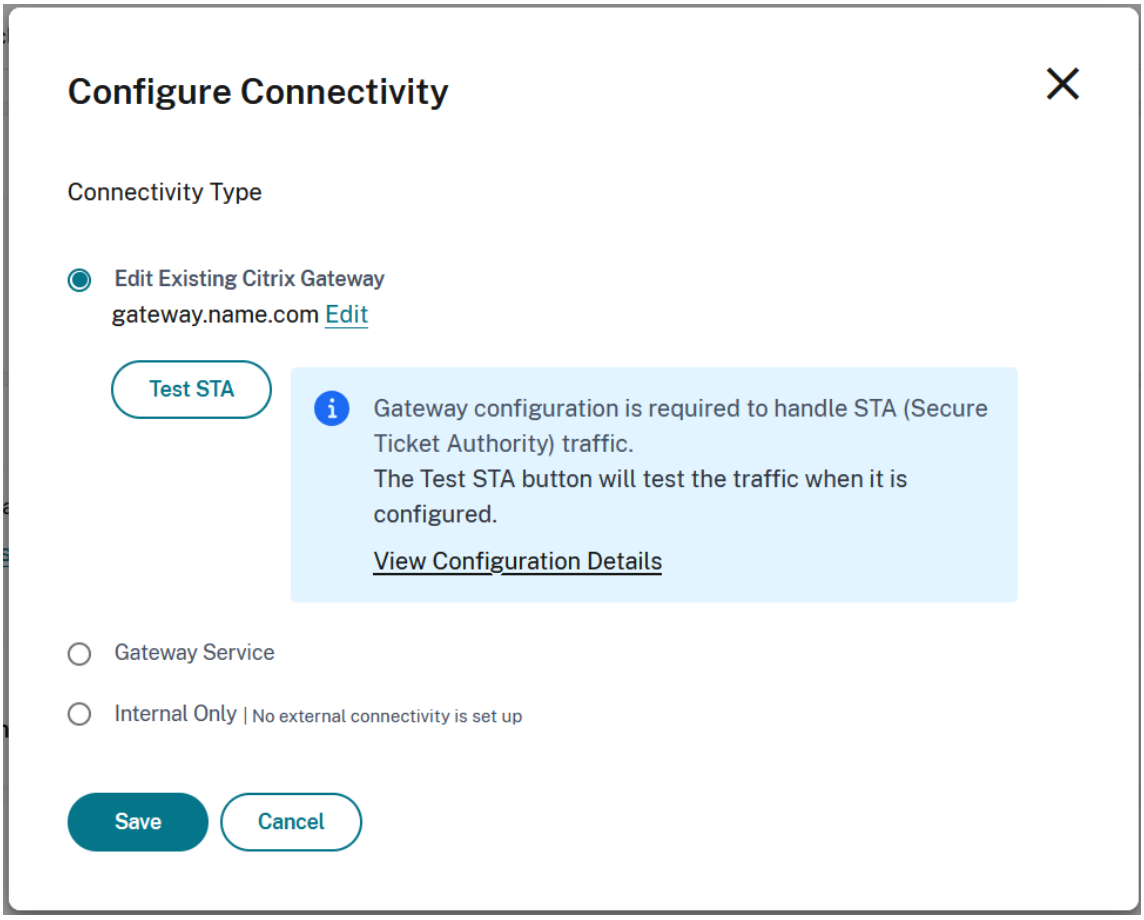
> Service continuity is not available when using a NetScaler Gateway. It is recommended that you use Citrix Gateway Service.

1. On the **Configure Connectivity** screen, select **Traditional Gateway**.




2. Enter the address of the gateway and select **Add**.

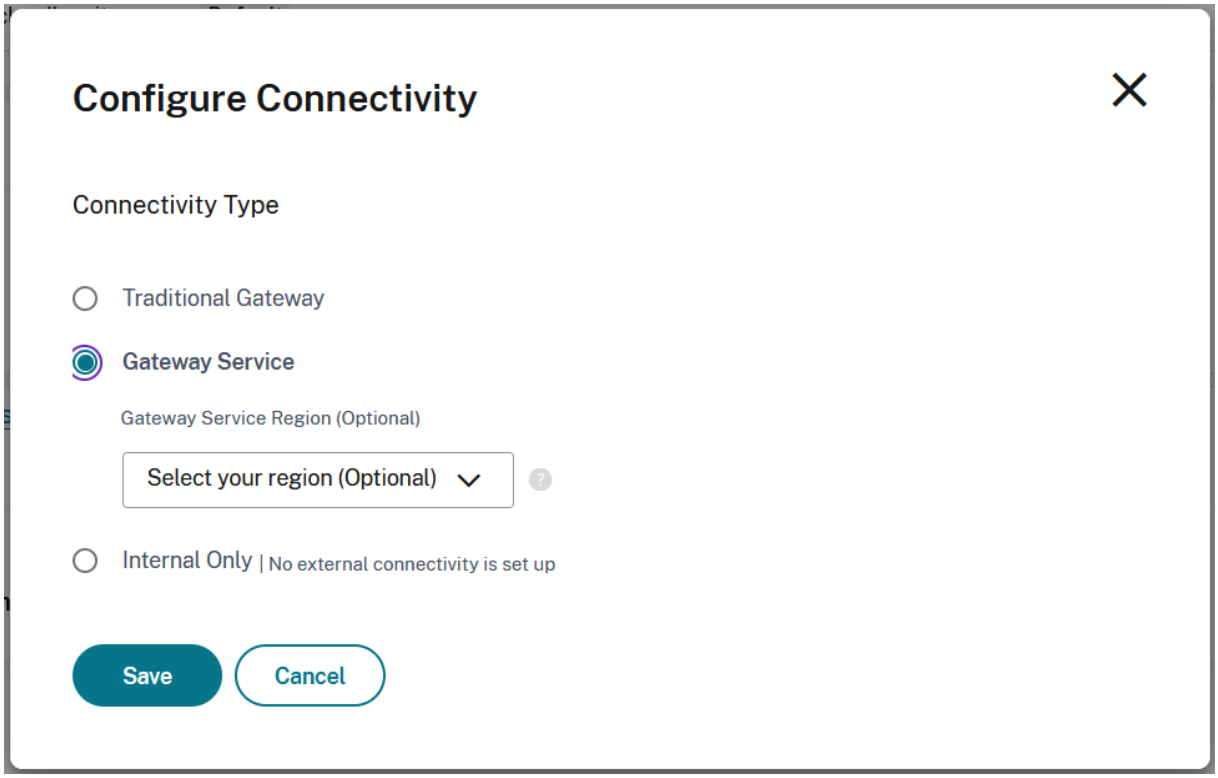



3. In the NetScaler Virtual Server configuration STA server list, add all of the Cloud Connectors for the resource location. Currently STA tickets are created by the cloud ticketing authority as long as the NetScaler Gateway can connect to one active Cloud Connector then it can reach the cloud ticketing authority. However in the future STA tickts will be created by a randomly assigned connector in the resource location so it is important that the NetScaler Gateway is configured with the complete list of all connectors in the resoure location.
4. Select **Test STA** to check connectivity.

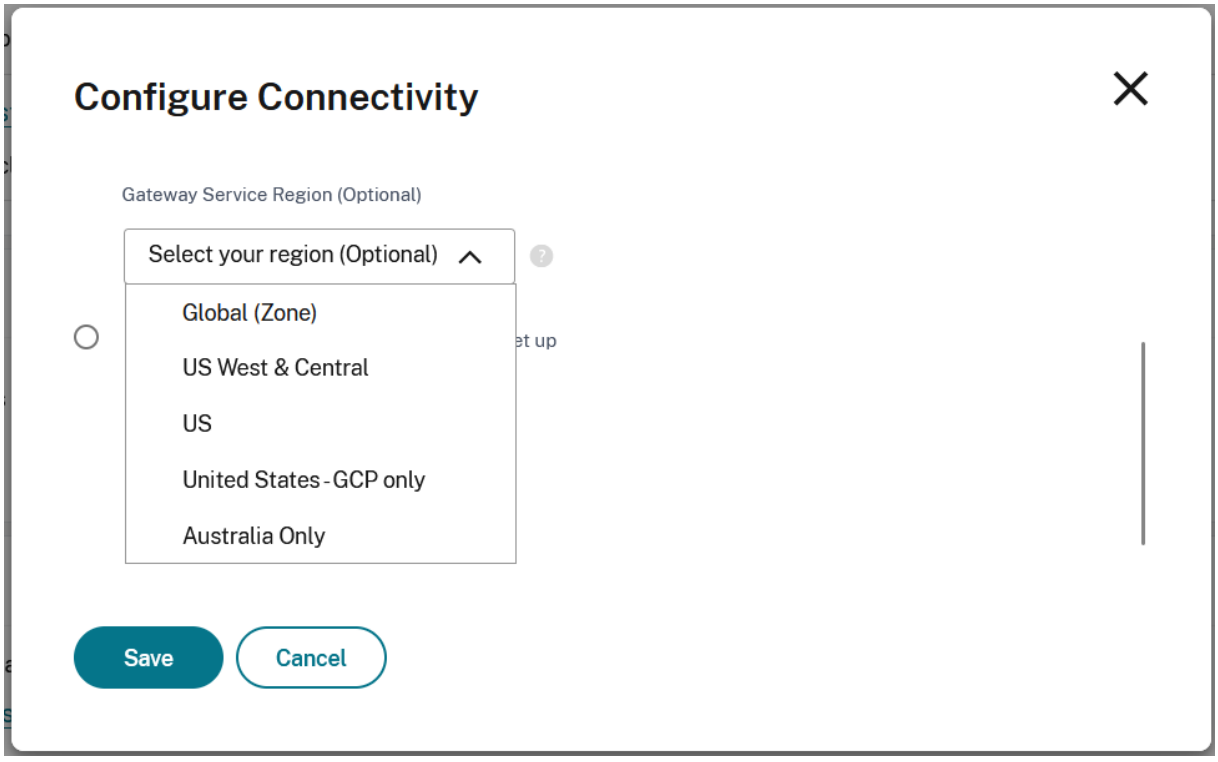
#### Gateway Service

You can use the Citrix Gateway Service to provide connectivity to resources without needing to deploy any infrastructure other than Cloud Connectors. Endpoints connect to one of the Citrix Gateway Service points of presence and HDX traffic is routed via the cloud connector to the VDA.



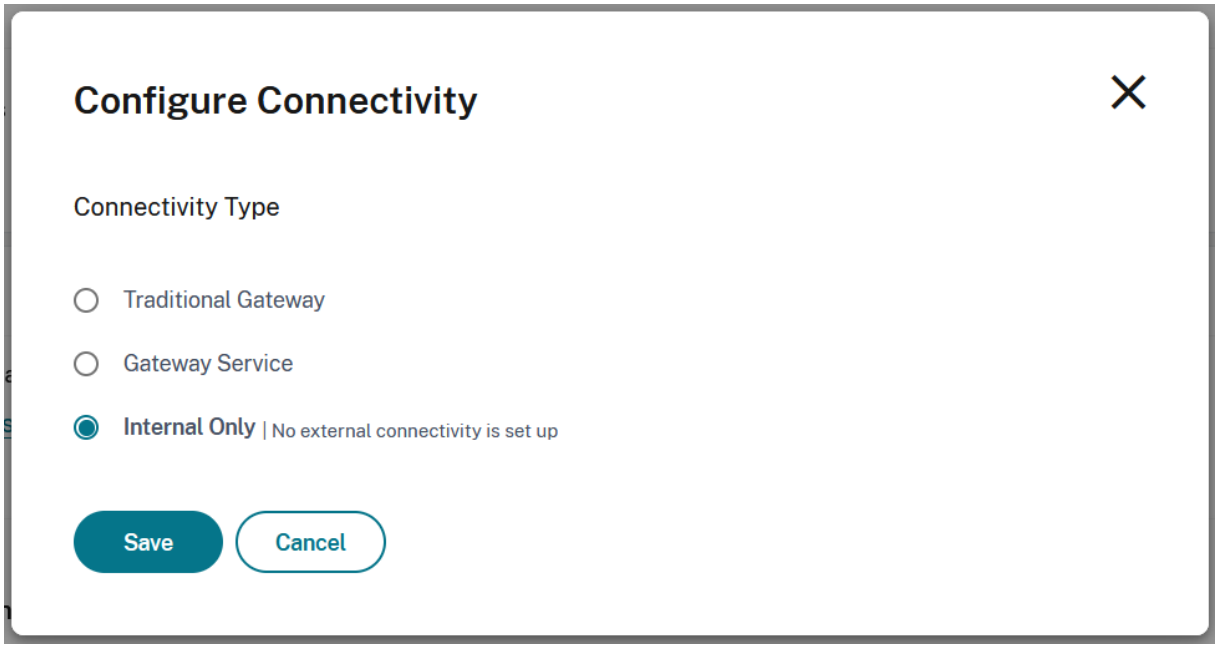

By default Citrix Gateway Service uses the point of presence nearer to the user. You can optionally choose a specific Gateway Service region.



**Internal only**

If you select **Internal only** then clients can only connect to resources if they have direct network connectivity.




### Connectivity options when Adaptive access is enabled

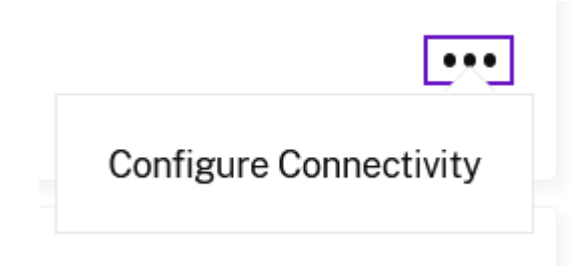
If Adaptive access is enabled, you can configure different connectivity depending on whether the device's public IP address maps to a Network location whose **Connectivity type** is **Internal** or **External**, or is **Undefined** (meaning it does not map to a Network location).

> **Notes:**
>
> - It is not possible to distinguish between different networks with the same public IP address. For instance if your corporate network and guest wi-fi both use the same public IP address, they will map to the same Network location so use the same configuration.
> - The HTML5 HDX client must connect to the VDA using a secure TLS connection. If an HTML5 HDX client tries to connect to a resource hosted on a VDA not configured for TLS, Citrix® StoreFront Cloud always uses the configuration specified for **Undefined** network locations, regardless of the device's actual location.
> - Regardless of the connectivity configuration, if you have enabled HDX direct, then the client will use a direct connection if possible.

To edit the connectivity options:

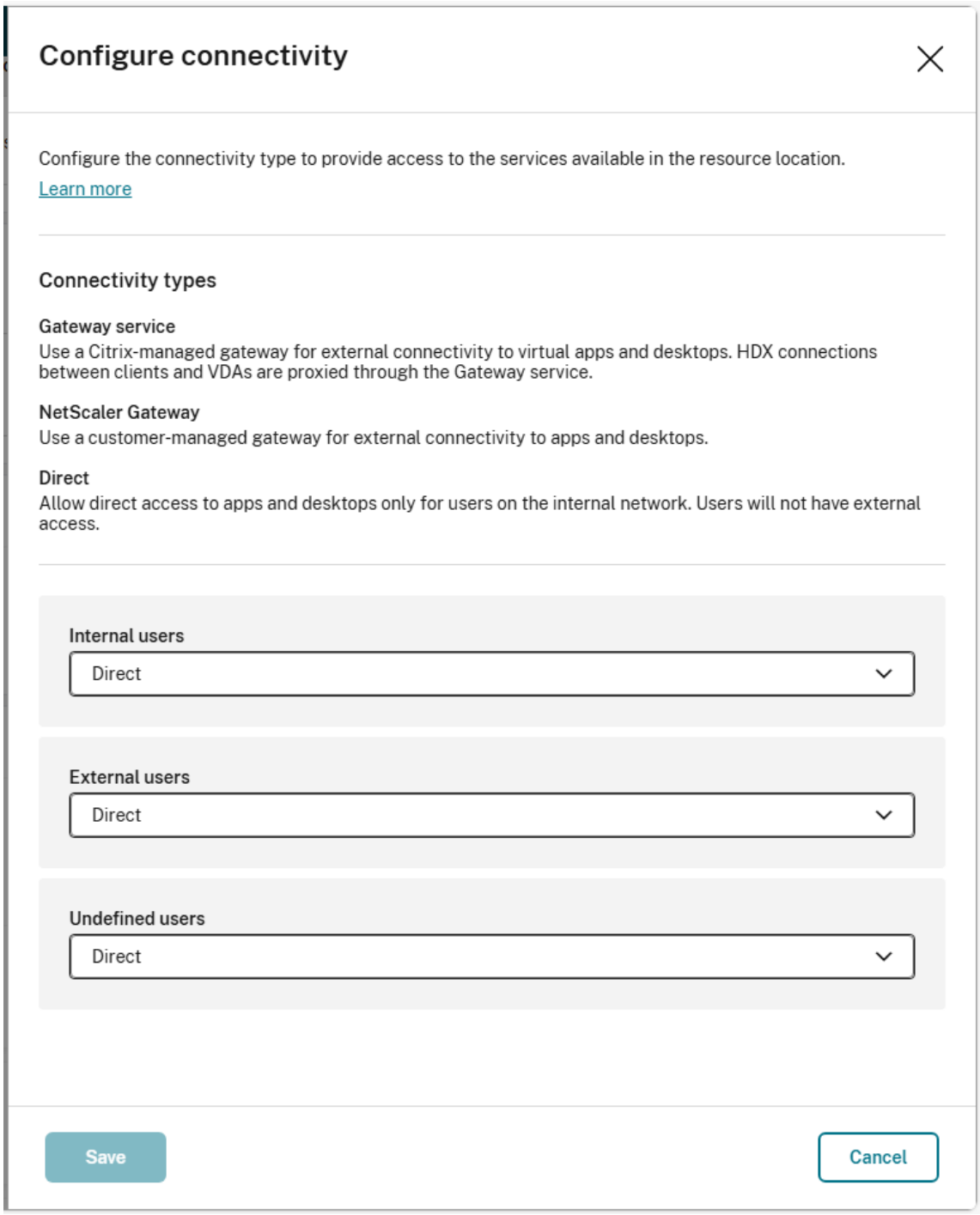
 

1. Select ... to open the menu




2. Select **Configure Connectivity**.




3. For each connectivity type, choose and configure the desired connectivity option.
   - NetScaler Gateway
   - Gateway Service
   - Direct
4. Select **Save**.

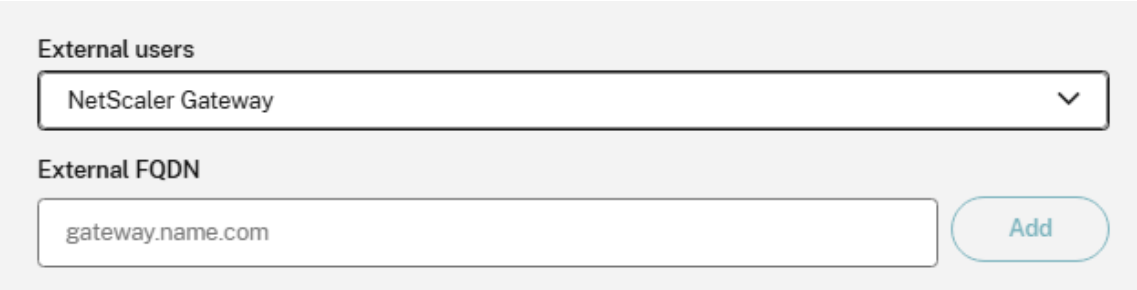
 

### NetScaler Gateway

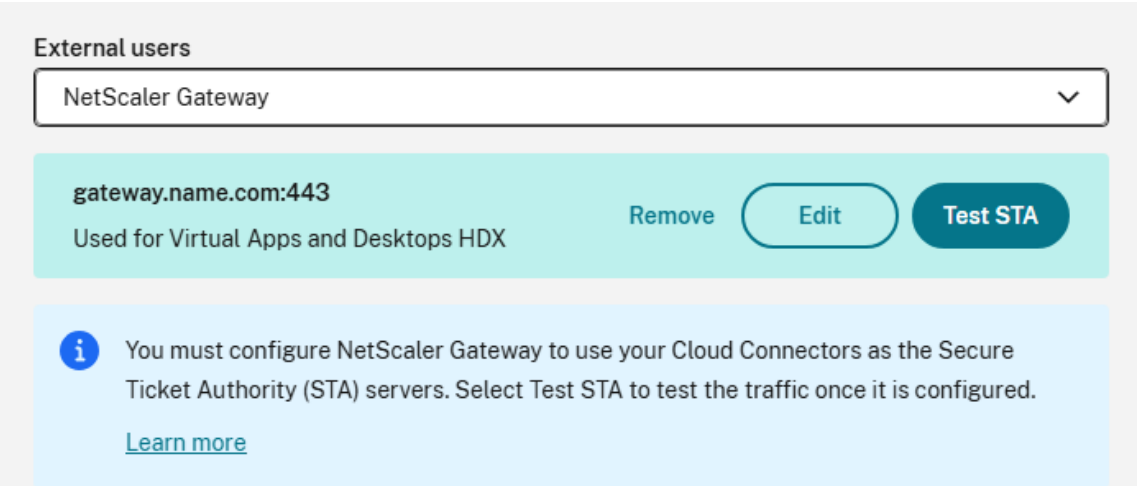
You can use a NetScaler gateway for HDX routing.

> **Warning:**
>
> There is no service continuity when using a NetScaler Gateway.

1. On the **Configure Connectivity** screen, select **NetScaler Gateway**.




2. Enter the address of the gateway and select **Add**.




3. In the NetScaler Virtual Server configuration STA server list, add all of the Cloud Connectors for the resource location. Currently STA tickets are created by the cloud ticketing authority as long as the NetScaler Gateway can connect to one active Cloud Connector then it can reach the cloud ticketing authority. However in the future STA tickets will be created by a randomly assigned connector in the resource location so it is important that the NetScaler Gateway is configured with the complete list of all connectors in the resource location.
4. Select **Test STA** to check connectivity.

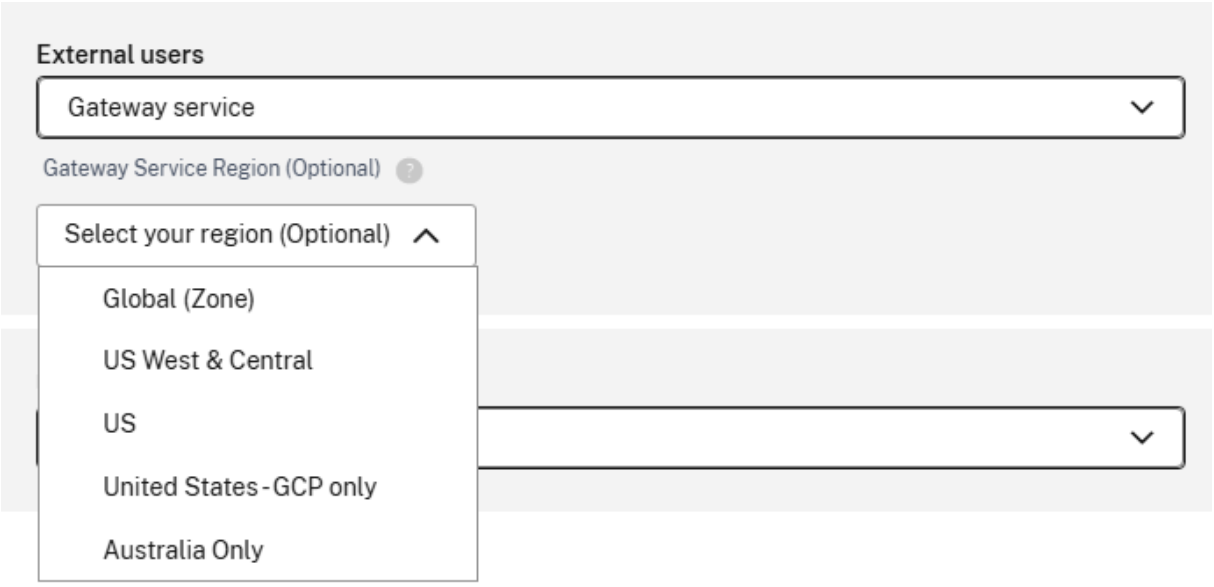
### Gateway Service

You can use the Citrix Gateway Service to provide connectivity to resources without needing to deploy any infrastructure other than Cloud Connectors. Endpoints connect to one of the Citrix Gateway

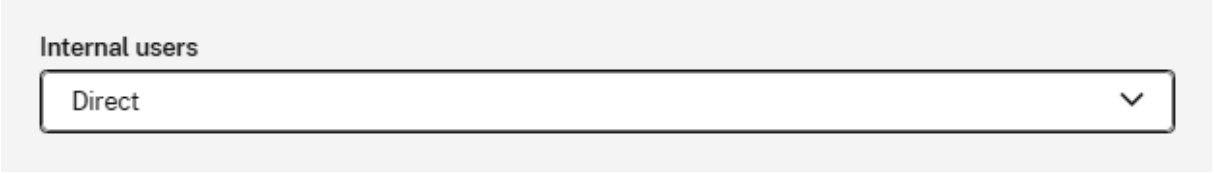
Service points of presence and HDX traffic is routed via the cloud connector to the VDA.


By default Citrix Gateway Service uses the point of presence nearer to the user. You can optionally choose a specific Gateway Service region.




**Direct**

If you select **Direct** then clients can only connect to resources if they have direct network connectivity.




## Troubleshooting

To verify that launches being routed as expected, use one of the following methods:

- View VDA connections through Monitor.
- Use ICA® file logging to verify the correct addressing of the client connection.

#### Citrix Montior

From Citrix Monitor, search for a user with an active session. In the **Session Details** section of the console, direct VDA connections display as UDP connections while gateway connections display as TCP connections.

If you don't see UDP on the DaaS Console then you must enable the HDX™ Adaptive Transport Policy for the VDAs.

#### ICA file logging

Enable ICA file logging on the client computer as described in Citrix Workspace app for Windows documentation. After launching sessions, examine the **Address** and **SSLProxyHost** entries in the logged ICA file.

**Direct VDA connections** For direct VDA connections, the **Address** property contains the VDA's IP address and port.

Here's an example of an ICA file when a client launches an application using the NLS:

```
[Notepad++ Cloud]
Address=;10.0.1.54:1494
SSLEnable=Off
```

The **SSLProxyHost** property isn't present in this file. This property is included only for launches through a gateway.

**Gateway connections** For gateway connections, the **Address** property contains the Citrix Cloud STA ticket, the **SSLEnable** property is set to **On**, and the **SSLProxyHost** property contains the gateway's FQDN and port.

Here's an example of an ICA file when a client has a connection through the Citrix Gateway service and launches an application:

```
[PowerShell ISE Cloud]
Address=;40;CWSSTA;027C02199068B33889A40C819A85CBB4
SSLEnable=On
SSLProxyHost=global.g.nssvcstaging.net:443
```

Here's an example of an ICA file when a client has a connection through an on-premises gateway and launches an application using an on-premises gateway that is configured within the resource location:

```
[PowerShell ISE Cloud]
Address=;40;CWSSTA;027C02199068B33889A40C819A85CBB5
SSLEnable=On
SSLProxyHost=onpremgateway.domain.com:443
```

> **Note:**
>
> On-premises gateway virtual servers that are used to launch virtual apps and desktops must be VPN virtual servers, not nFactor authentication virtual servers. The nFactor authentication virtual servers are for user authentication only and don't proxy resource HDX and ICA launch traffic.

#### VDA launch failures

If VDA sessions are failing to launch, verify you're using public IP address ranges from the correct network. When configuring your network locations, you must use the public IP address ranges of the network where your internal users are connecting from to reach the Internet.

#### Internal VDA launches still routed through the gateway

If VDA sessions launched internally are still being routed through the gateway as if they were external sessions, verify you're using the correct public IP address that your internal users are connecting from to reach their store. The public IP address listed in the NLS site must correspond to the address that the client launching the resources uses to access the Internet. To obtain the correct public IP address for the client, log on to the client machine, visit a search engine, and enter "what is my ip"in the search bar.

All clients that launch resources within the same office location typically access the Internet using the same network egress public IP address. These clients must have an internet network route to the subnets where the VDAs reside, which isn't blocked by a firewall.

## Configure Authentication

June 22, 2026

As an administrator, you can choose to have your end users authenticate to their stores using one of the following authentication methods:

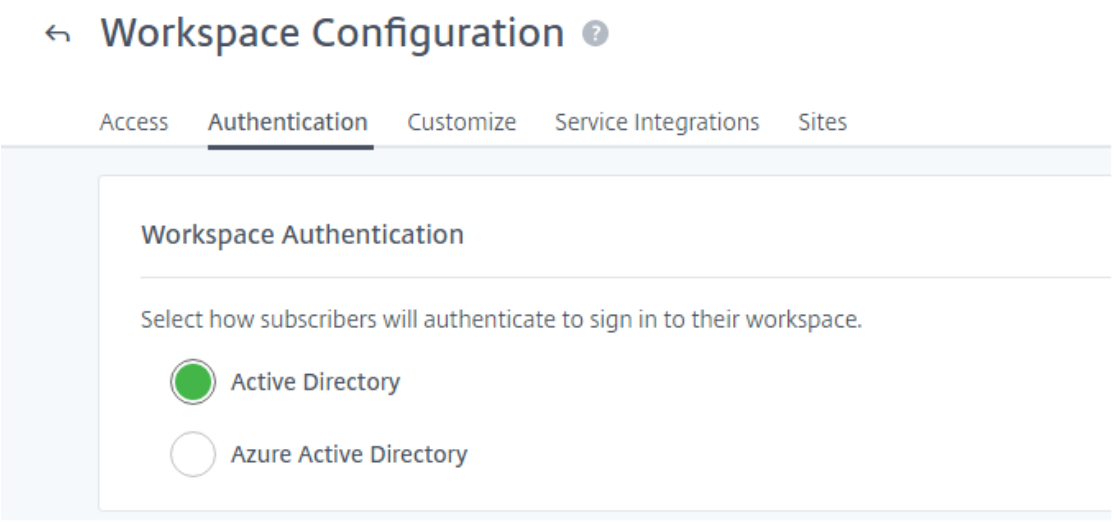
 

- Active Directory (AD)
- Active Directory plus token
- Azure Active Directory (AAD)
- Citrix Gateway
- Google
- Okta
- SAML 2.0

Citrix® StoreFront Cloud also supports single sign-on to your virtual apps and desktops. When the user enters their Active Directory credentials, store can use these to provide SSO to resources. When using other IdPs, store can use Citrix Federated Authentication Service (FAS) to provide single sign-on (SSO) to resources.

### Choose or change authentication methods

1. Define one or more identity providers in **Identity and Access Management**. For instructions, visit Identity and access management.
2. Choose or change how end users authenticate to their store in **StoreFront Cloud > Authentication > store Authentication**.




> **Important:**
>
> Switching authentication modes can take up to five minutes and causes an outage to your end users during that time. The outage affects access to the store and has no impact on HDX™ sessions. Citrix recommends limiting changes to periods of low usage. If you do have end users logged on to their store using a browser or Citrix Workspace app, advise them to close the browser or exit the app. After waiting approximately five minutes, they can sign in again using

> the new authentication method.

### Active Directory (AD)

By default, Citrix Cloud™ uses Active Directory (AD) to manage end user authentication to stores.

To use AD, you must have at least two Citrix Cloud Connectors installed in the on-premises AD domain. For more information on installing the Cloud Connector, see Cloud Connector Installation.

#### Single Sign-on to VDAs with AD

When using AD authentication, store provides SSO capability when launching AD joined virtual apps and desktops.

### Active Directory (AD) plus token

For greater security, Citrix® StoreFront Cloud supports a time-based token as a second factor of authentication to AD sign-in.

For each login, store prompts end users to enter a token from an authentication app on their enrolled device. Before signing in, end users must enroll their device with an authentication app that follows the Time-Based One-Time Password (TOTP) standard, such as Citrix SSO. Currently, end users can enroll only one device at a time.

For more information, see Tech Insight: Authentication - TOTP and Tech Insight: Authentication - Push.

#### Single Sign-on to VDAs with AD plus token

When using AD plus token authentication, store provides SSO capability when launching AD joined virtual apps and desktops.

#### Requirements for AD plus token

Active Directory plus token authentication has the following requirements:

- A connection between Active Directory and Citrix Cloud, with at least two Cloud Connectors installed in your on-premises environment. For requirements and instructions, see Connect Active Directory to Citrix Cloud.
- **Active Directory + Token** authentication enabled in the **Identity and Access Management** page. For information, see To enable Active Directory plus token authentication.

- End user access to email to enroll devices.
- A device on which to download the authentication app.

### First-time enrollment

End users enroll their devices using the enrollment process described in Register devices for two-factor authentication.

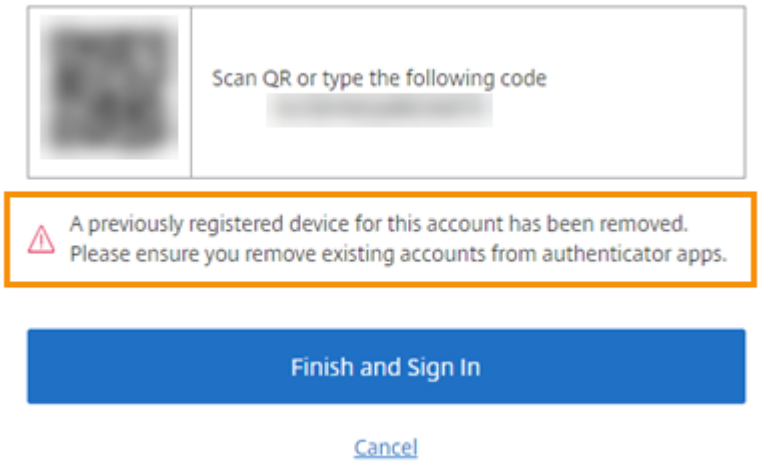
During first-time sign-in to store, end users follow the prompts to download the Citrix SSO app. The Citrix SSO app generates a unique one-time password on an enrolled device every 30 seconds.

> **Important:**
>
> During the device enrollment process, end users receive an email with a temporary verification code. This temporary code is used only to enroll the end user's device. Using this temporary code as a token for signing in to a store with two-factor authentication isn't supported. Only verification codes that are generated from an authentication app on an enrolled device are supported tokens for two-factor authentication.

### Re-enroll a device

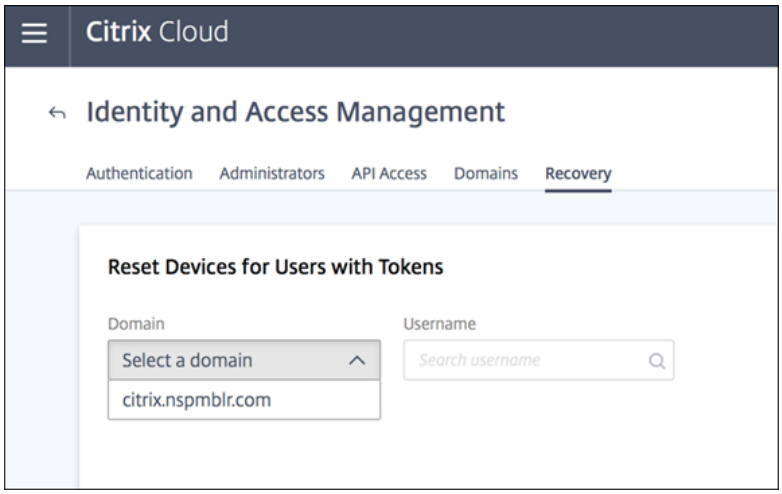
If an end user no longer has their enrolled device or needs to re-enroll it (for example, after erasing content from the device), store provides the following options:

- End users can re-enroll their devices using the same enrollment process described in Register devices for two-factor authentication. Because end users can enroll only one device at a time, enrolling a new device or re-enrolling an existing device removes the previous device registration.



- Administrators can search for end users by Active Directory name and reset their device. To do that, go to **Identity and Access Management > Recovery**. During the next sign-on to store, the end user experiences the first-time enrollment steps.




### Azure Active Directory

Use of Azure Active Directory (AD) to manage end user authentication to stores has the following requirements:

- Microsoft Entra ID (formerly Microsoft Azure AD) with a user who has global administrator permissions. For more information on the Microsoft Entra ID applications and permissions that Citrix Cloud uses, see Azure Active Directory Permissions for Citrix Cloud.
- A Citrix Cloud Connector™ installed in the on-premises AD domain. The machine must also be joined to the domain that is syncing to Microsoft Entra ID.
- VDA version 7.15.2000 LTSR CU VDA or 7.18 current release VDA or higher.
- A connection between Microsoft Entra ID and Citrix Cloud. For information, see Connect Azure Active Directory to Citrix Cloud.
- Any version of Citrix Workspace app. If using legacy Citrix Receiver™ then you must use the following minimum versions:
  - Citrix Receiver for Windows 4.11 CR or 4.9 LTSR CU2 or higher
  - Citrix Receiver for Linux 13.8
  - Citrix Receiver for Android 3.13 and later

When syncing your Active Directory to Microsoft Entra ID, the UPN and SID entries must be included in the sync. If these entries aren't synchronized, certain workflows in Citrix® StoreFront Cloud fail.

> **Warning:**
>
> - If you're using Microsoft Entra ID, don't make the registry change described in CTX225819.

> Making this change might cause session launch failures for Microsoft Entra ID users.
> - Adding a group as a member of another group (nesting) is supported with the `DSAuthAzureAdNestedGroups` feature enabled. You can enable `DSAuthAzureAdNestedGroups` by submitting a request to Citrix Support.

After enabling Microsoft Entra ID authentication:

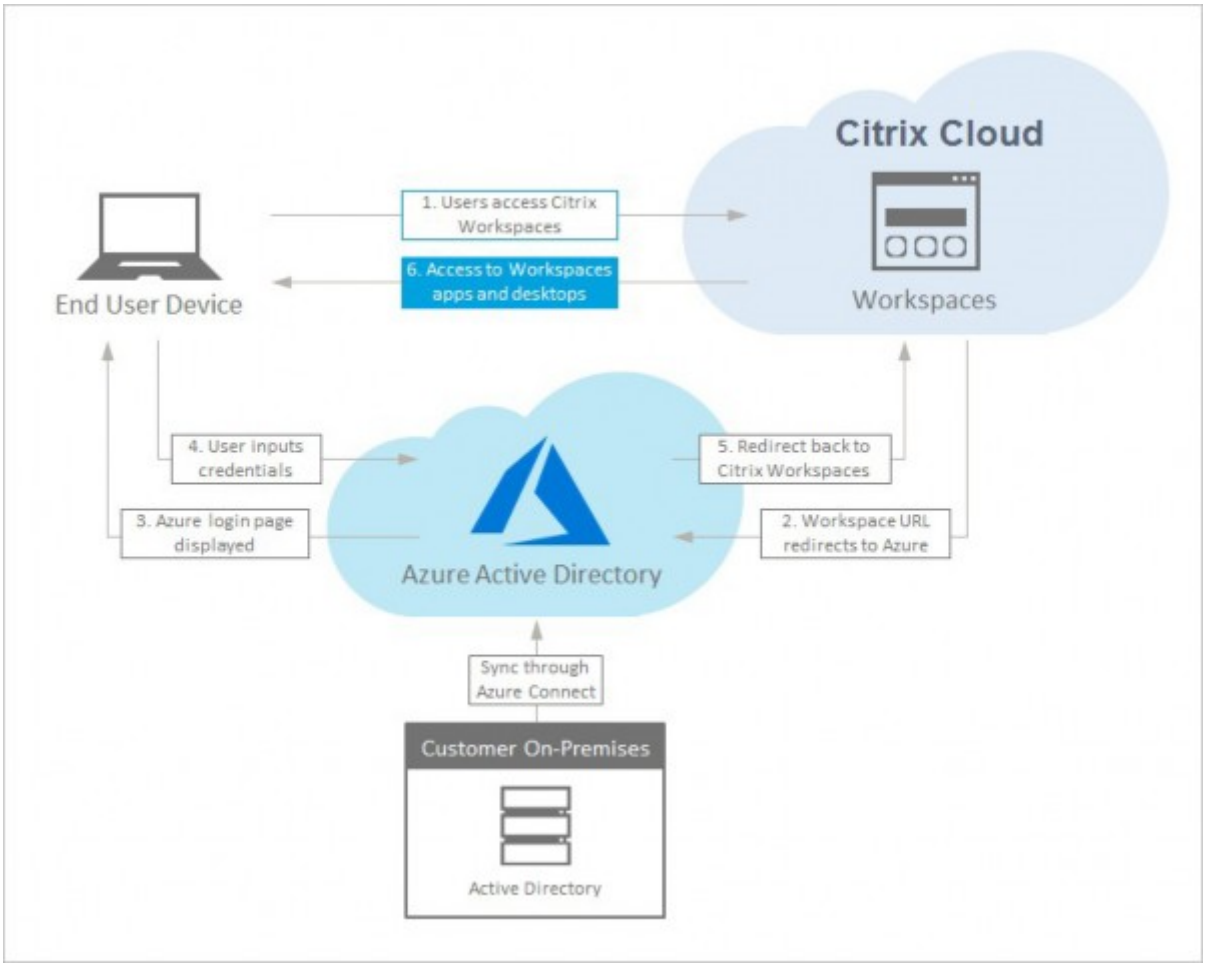
- **Added security:** For security, users are prompted to sign in again when launching an app or a desktop. The password information flows directly from user's device to the VDA that is hosting the session.
- **Sign-in experience:** Microsoft Entra ID authentication provides federated sign-in, not single sign-on (SSO). End users sign in from an Azure sign-in page, and might have to authenticate again when opening Citrix DaaS.

For SSO, enable the Citrix Federated Authentication Service in Citrix Cloud. See Enable single sign-on for stores with Citrix Federated Authentication Service for more information.

You can customize the sign-in experience for Microsoft Entra ID. For information, see the Microsoft documentation. Any sign-in customizations (the logo) made in Citrix® StoreFront Cloud do not affect the Microsoft Entra ID sign-in experience.

The following diagram shows the sequence of Microsoft Entra ID authentication.




## Sign-out experience

Use **Settings > Log Off** to complete the sign-out process from store and Microsoft Entra ID. If end users close the browser instead of using the **Log Off** option, they might remain signed in to Microsoft Entra ID.

> **Important:**
>
> If the log in times out in the browser due to inactivity, end users remain signed in to Microsoft Entra ID. This prevents a timeout timeout from forcing other Microsoft Entra ID applications to close.

### Single Sign-on to VDAs with EntraId

If the IdP is Entra ID then you can use Entra ID SSO to VDAs. For other cases, to enable Single Sign on to VDAs you must use FAS.

### Citrix Gateway

You can use an on-premises Citrix Gateway as an identity provider to manage end user authentication to stores. For more information, see Tech Insight: Authentication - Citrix Gateway.

#### Requirements for Citrix Gateway

Citrix Gateway authentication has the following requirements:

- A connection between your Active Directory and Citrix Cloud. For requirements and instructions, see Connect Active Directory to Citrix Cloud.
- End users must be Active Directory users to sign in to their stores.
- If you're performing federation, your AD users must be synchronized to the federation provider. Citrix Cloud requires the AD attributes to allow users to sign in successfully.
- An on-premises Citrix Gateway:
  - Citrix Gateway 12.1 54.13 Advanced edition or later
  - Citrix Gateway 13.0 41.20 Advanced edition or later
- **Citrix Gateway** authentication enabled in the **Identity and Access Management** page. This generates the client ID, secret, and redirect URL required to create the connection between Citrix Cloud and your on-premises Gateway.
- On the Gateway, an OAuth IdP authentication policy is configured using the generated client ID, secret, and redirect URL.

For more information, see Connect an on-premises Citrix Gateway as an identity provider to Citrix Cloud.

#### End user experience of Citrix Gateway

When authentication with Citrix Gateway is enabled, end users experience the following workflow:

1. The end user navigates to the store URL in their browser or launches Workspace app.
2. The end user is redirected to the Citrix Gateway logon page and is authenticated using any method configured on the Gateway. This method can be MFA, federation, conditional access policies, and so on. You can customize the Gateway logon page so that it looks the same as the store sign-in page using the steps described in CTX258331.
3. After successful authentication, the end user's workspace appears.

### Single sign-on with Gateway

Depending on how you configure Citrix Gateway, you might not need FAS for SSO to DaaS. For more information on configuring Citrix Gateway, visit Create an OAuth IdP policy on the on-premises Citrix Gateway.

### Google

You can use Google as an identity provider for end user authentication to stores.

#### Requirements for Google

- A connection between your on-premises Active Directory and Google Cloud.
- A developer account with access to the Google Cloud Platform console. This account is required for creating a service account and key, and enabling the Admin SDK API.
- An administrator account with access to the Google store Admin console. This account is required for configuring domain-wide delegation and a read-only API user account.
- A connection between your on-premises Active Directory domain and Citrix Cloud, with **Google** authentication enabled in the **Identity and Access Management** page. To create this connection, at least two Cloud Connectors are required in your resource location.

For more information, see Connect Google as an identity provider to Citrix Cloud.

#### End user experience with Google

When authentication with Google is enabled, end users experience the following workflow:

1. The end user navigates to the store URL in their browser or launches the Workspace app.
2. The end user is redirected to the Google sign-in page and is authenticated using the method configured in Google Cloud (for example, multifactor authentication, conditional access policies, and so on).
3. After successful authentication, the end user's workspace appears.

#### Single Sign-on to VDAs with Google

When using Google authentication, to enable Single Sign on to VDAs you must use FAS.

## Okta

You can use Okta as an identity provider for end user authentication to stores. For more information, see Tech Insight: Authentication - Okta.

### Requirements for Okta

Okta authentication has the following requirements:

- A connection between your on-premises Active Directory and your Okta organization.
- An Okta OIDC web application configured for use with Citrix Cloud. To connect Citrix Cloud to your Okta organization, you must supply the Client ID and Client Secret associated with this application.
- A connection between your on-premises Active Directory domain and Citrix Cloud, with **Okta** authentication enabled in the **Identity and Access Management** page.

For more information, see Connect Okta as an identity provider to Citrix Cloud.

### End user experience with Okta

When authentication with Okta is enabled, end users experience the following workflow:

1. The end user navigates to the store URL in their browser or launches the Workspace app.
2. The end user is redirected to the Okta sign-in page and is authenticated using the method configured in Okta (for example, multifactor authentication, conditional access policies, and so on).
3. After successful authentication, the end user's workspace appears.

### Single Sign-on to VDAs with Okta

When using Okta authentication, to enable Single Sign on to VDAs you must use FAS.

## SAML 2.0

You can use SAML 2.0 to connect an IdP for end user authentication to stores.

### Requirements for SAML 2.0

SAML authentication has the following requirements:

- SAML provider that supports SAML 2.0.

- On-premises Active Directory domain.
- Two Cloud Connectors deployed to a resource location and joined to your on-premises AD domain.
- AD integration with your SAML provider.

For more information about configuring SAML authentication for stores, see Connect SAML as an identity provider to Citrix Cloud.

#### End user experience with SAML 2.0

1. The end user navigates to the store URL in their browser or launches Citrix Workspace app.
2. The end user is redirected to the SAML identity provider sign-in page for their organization. The end user authenticates with the mechanism configured for the SAML identity provider, such as multifactor authentication or conditional access policies.
3. After successful authentication, the end user's workspace appears.

#### Single Sign-on to VDAs with SAML 2.0

If the IdP is Entra ID then you can use Entra ID SSO to VDAs. For other cases, to enable Single Sign on to VDAs you must use FAS.

### Citrix Federated Authentication Service (FAS)

You can deploy Citrix Federated Authentication Service (FAS) for single sign-on (SSO) to Citrix DaaS. Without FAS, end users using a federated identity provider are prompted to enter their credentials more than once to access their virtual apps and desktops.

For more information, see Citrix Federated Authentication Service (FAS).

### Entra ID SSO to VDAs

If where the user has authenticated using Entra ID, Citrix® StoreFront Cloud supports using the Entra ID session to authenticate to the VDAs. For more information, see Microsoft Entra single sign-on.

This functionality is disabled by default and should only be enabled once you have completed the rest of the configuration, otherwise users may experience delayed or failed launches. To enable it, use the PowerShell modules version 1.0.6.

```
Set-StoreConfigurations -StoreUrl "https://<yourstore>.cloud.com" -
    ClientId "<clientId>" -ClientSecret "<clientSecret>" -
    AzureAdSsoEnabled $True
```

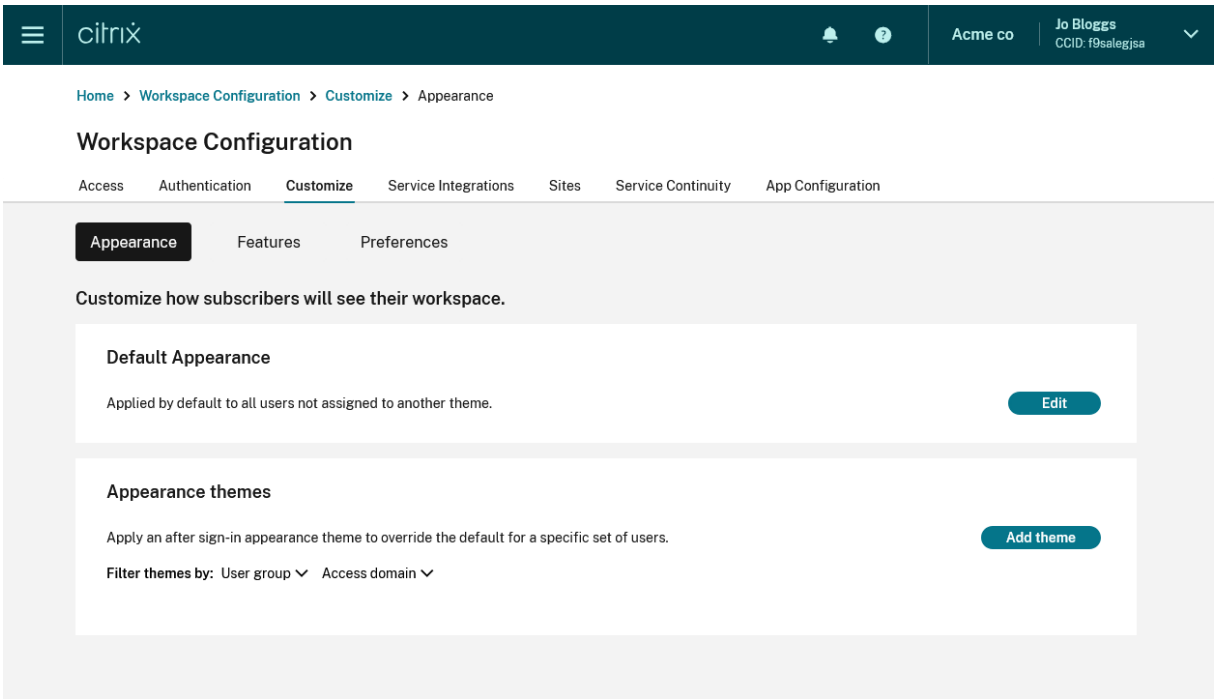
### More information

- Tech Brief: Workspace Single Sign-On

## Customize your store experience

June 22, 2026

To customize the store, from the menu open **StoreFront Cloud** then the **Customize** tab.




### Appearance

To customize your store with your own logos and colors, go to the **Appearance** tab. For more information, see Customize the appearance of stores.

### Features

To customize which feature your users have access to, go to the **Features** tab. For more information, see Enable and disable features.

### Preferences

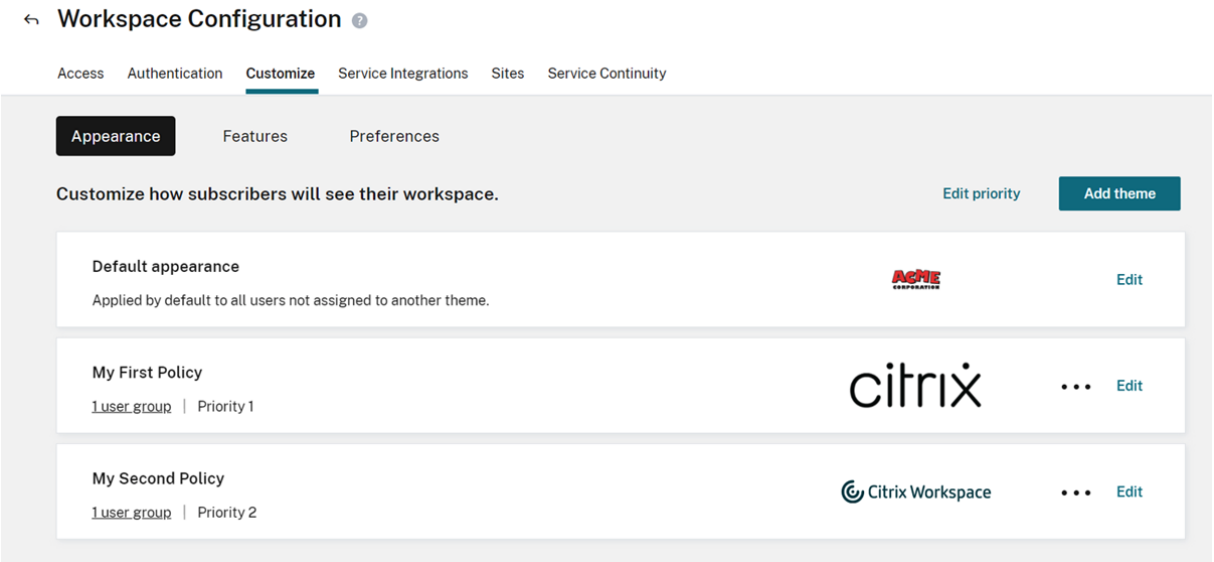
To modify other aspects of behavior, appearance, and configure access methods for the store, apps, and desktops, go to the **Preferences** tab. For more information, see the following pages:

- Custom announcements
- Allow end users to change their account password
- Pinned links
- User interface settings
- Store sessions
- Store access
- Log in dialog

## Customize the appearance of stores

June 22, 2026

You can create themes to customize the logos and colors of your store to match your corporate branding guidelines. You can configure a default theme along with additional theme overrides that apply to specific stores or user groups. To view and modify the appearance, from **StoreFront Cloud** select **Customize** then **Appearance**.



## Supported customizations

### Sign in appearance

For the sign-in page, you can only replace the logo. The rest of the sign-in page, including the colors, isn't affected.

> **Note:**
>
> Changes to the sign-in logo don't impact users who authenticate to their store using third-party identity providers, such as Microsoft Entra ID and Okta.
>
> For information on how to customize an Microsoft Entra ID sign-in page, see the Microsoft documentation. For information on how to customize the sign-in page hosted by Okta, see the Okta Developer documentation.

You can also customize the on-premises Citrix Gateway sign-in page, configured in the Citrix ADC appliance rather than in **StoreFront Cloud**. For more information, see the Support Knowledge Center article.

### After log in appearance

You can customize the following elements

| Item | Description |
|---|---|
| Logo | The logo displayed in the banner at the top of the screen |
| Banner color | The color of the banner at the top of the screen |
| Banner text and icon color | The color of the activity manager and profile icons in the banner |
| Accent color | The color used to highlight selected items and for buttons |

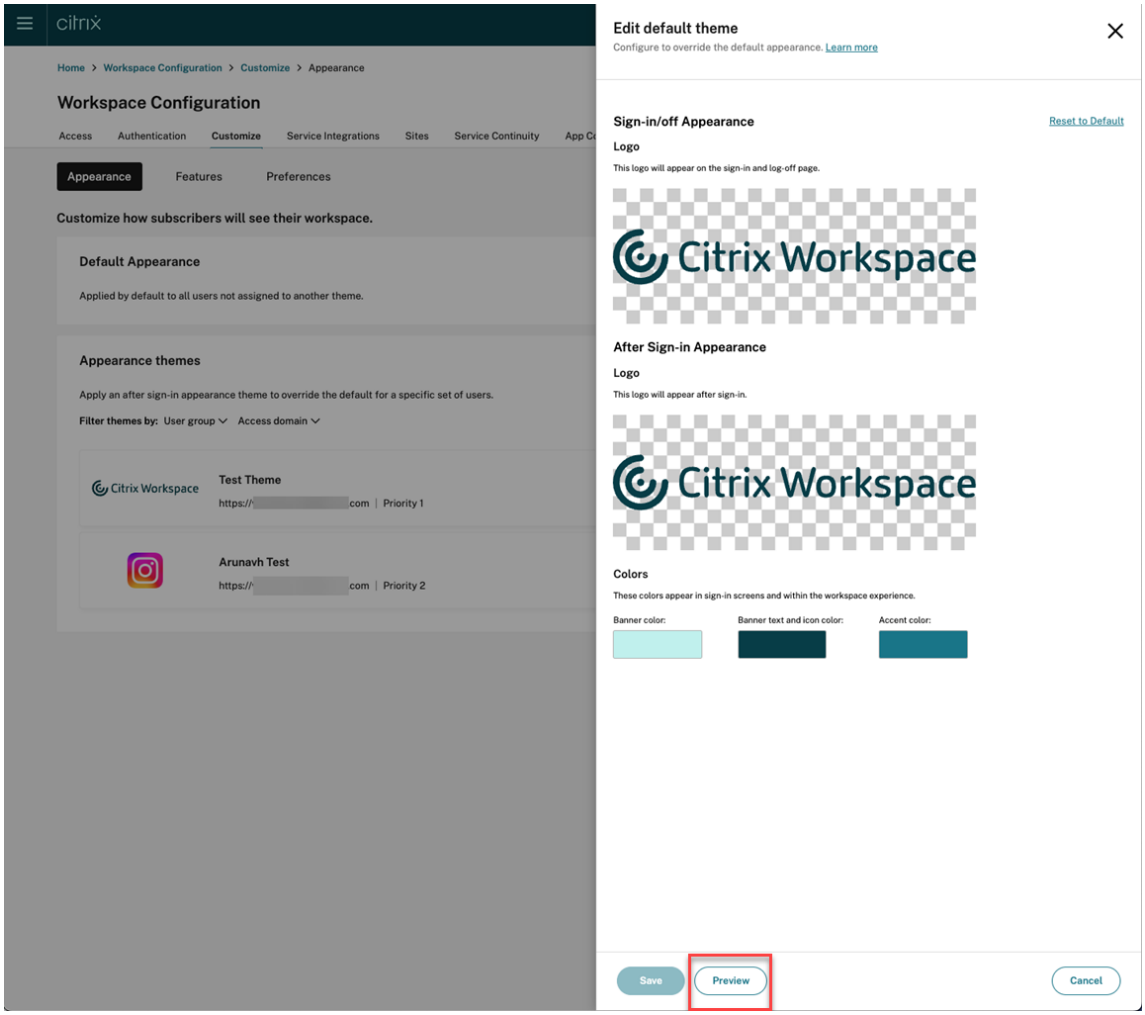
## Edit default theme

The default theme is used when no other theme applies. It also includes the log in screen logo which cannot be overridden.

To modify the default theme:

1. In the **Default Appearance** card, select **Edit**.




2. In the Sign-in/off Appearance section, optionally drag drop an image file to use as a logo. The logo should be 480 x 120 pixels, up to 2 MB size and have a file extension of JPEG, JPG, or PNG.
3. In the After Sign-in Appearance section, optionally drop drop an image file to use as a logo. The logo should be 340 x 80 pixels, up to 2 MB and have a file extension of JPEG, JPG, or PNG.
4. Click on the colors to change them. Either choose from the color picker or enter the color value. You can switch between hex, HSL and RGB values.
5. To preview the theme end users will see it, select **Preview**.
6. Select **Save**.

For users using a web browser, the change apply the next time the user logs in or refreshes the page. For users using Citrix Workspace™ app, changes take around five minutes to apply.

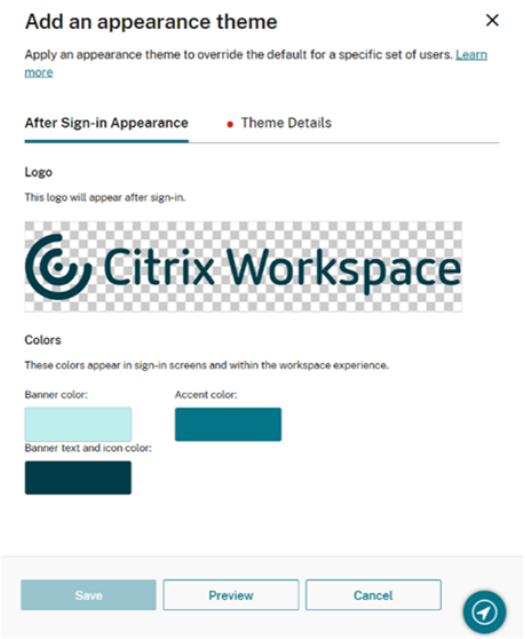
### Custom themes

You can configure and prioritize additional themes that apply to specific stores and user groups.

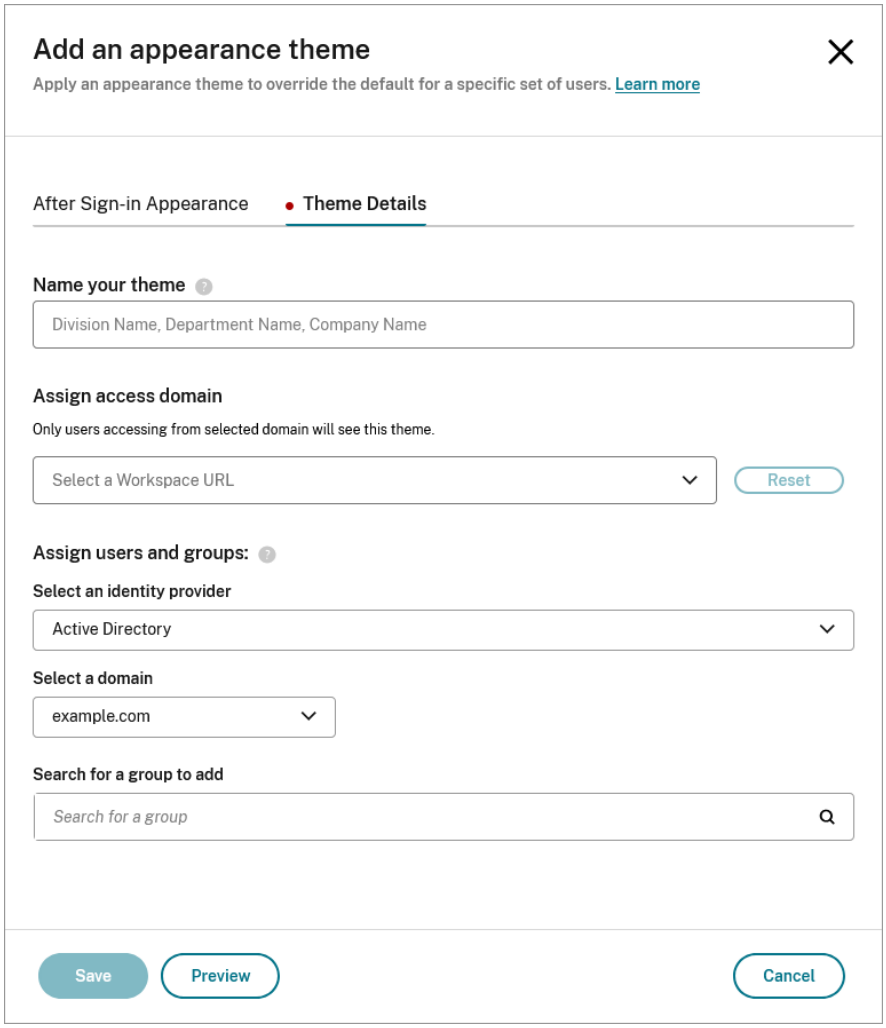
### Add custom theme

1. Press **Add theme**.




2. Configure your custom theme, in the same way as the default theme.
3. Select the **Theme Details** tab.

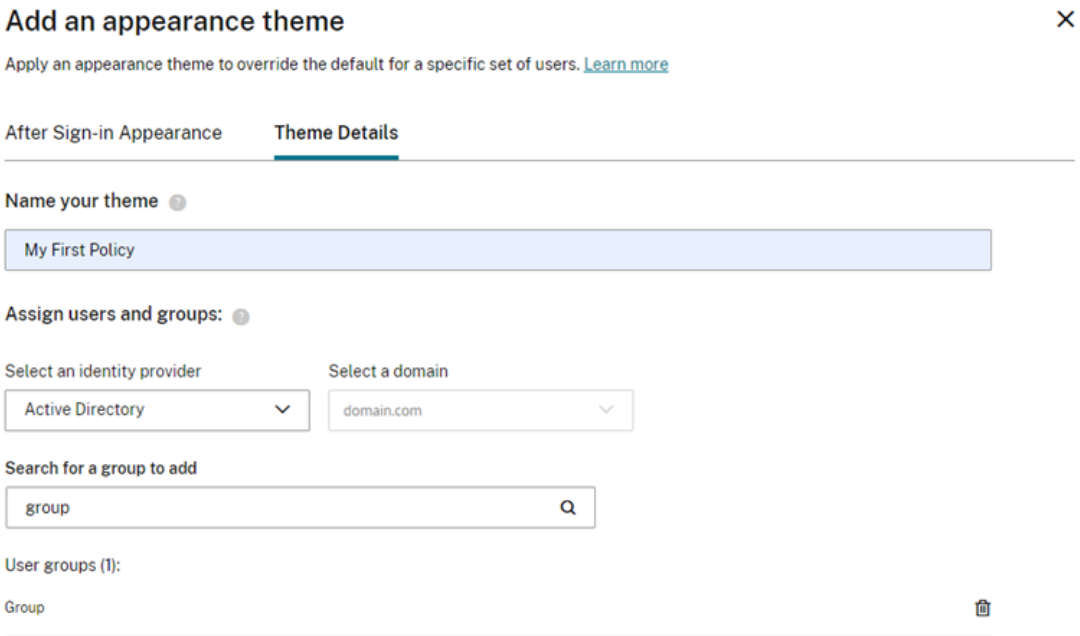
 




4. Enter a name for the theme.
5. Optionally specify which store the theme applies to.
6. Assign user groups to the theme:

    a) Select an identity provider, and its domain if prompted.
    b) Search for the user group that you want to add to the custom theme.
    c) Select the plus sign (**+**) button next to that group.
    d) Repeat this process for each group that you want to use your theme.




7. Optionally select **Preview** to see how your store looks to your end-users.
8. Press **Save**.

### Edit custom theme

1. On the theme card, select **Edit**.
2. Make changes as required.
3. Select **Save**.

### Delete custom theme

1. On the theme card, select **...** to open the menu.
2. Select **Delete**.
3. On the confirmation window, select **Delete**.

### Prioritize custom themes

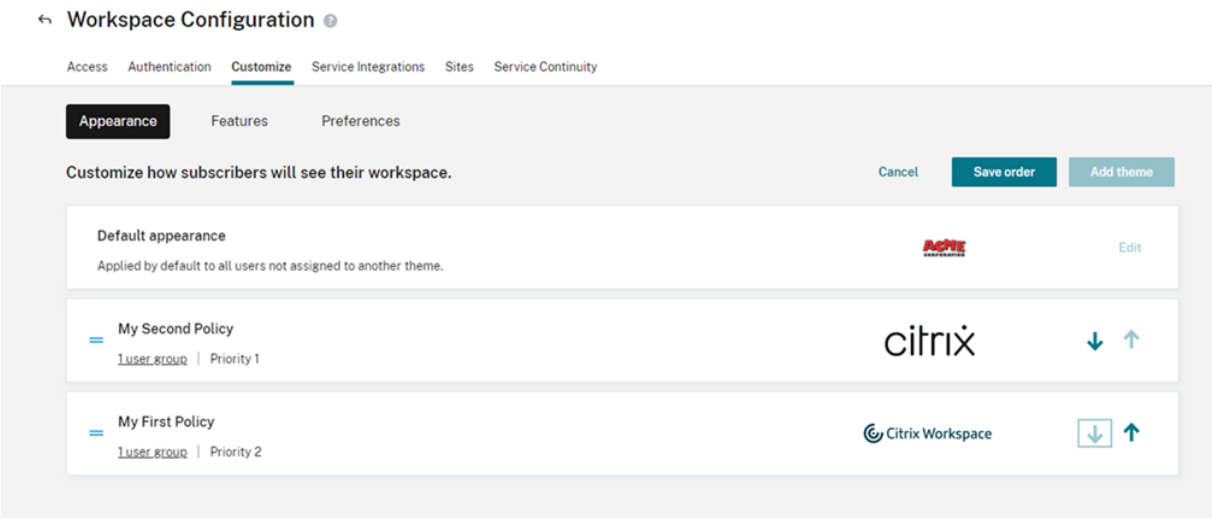
A user might belong to more than one user group, each of which might match to a different theme. You can define the order of precedence of themes. The first theme that matches the user's store and group applies. If no other themes apply then users see the default theme.

1. Select **Edit priority** at the top right of the list of themes, next to **Add theme**.
2. You can reorder the priority of themes in one of two ways:

- Use the arrows on the right-hand side of each theme.
- Drag individual themes up and down the list using the handle on the left-hand side of the card.

3. Once you've reordered your items, select **Save order**.

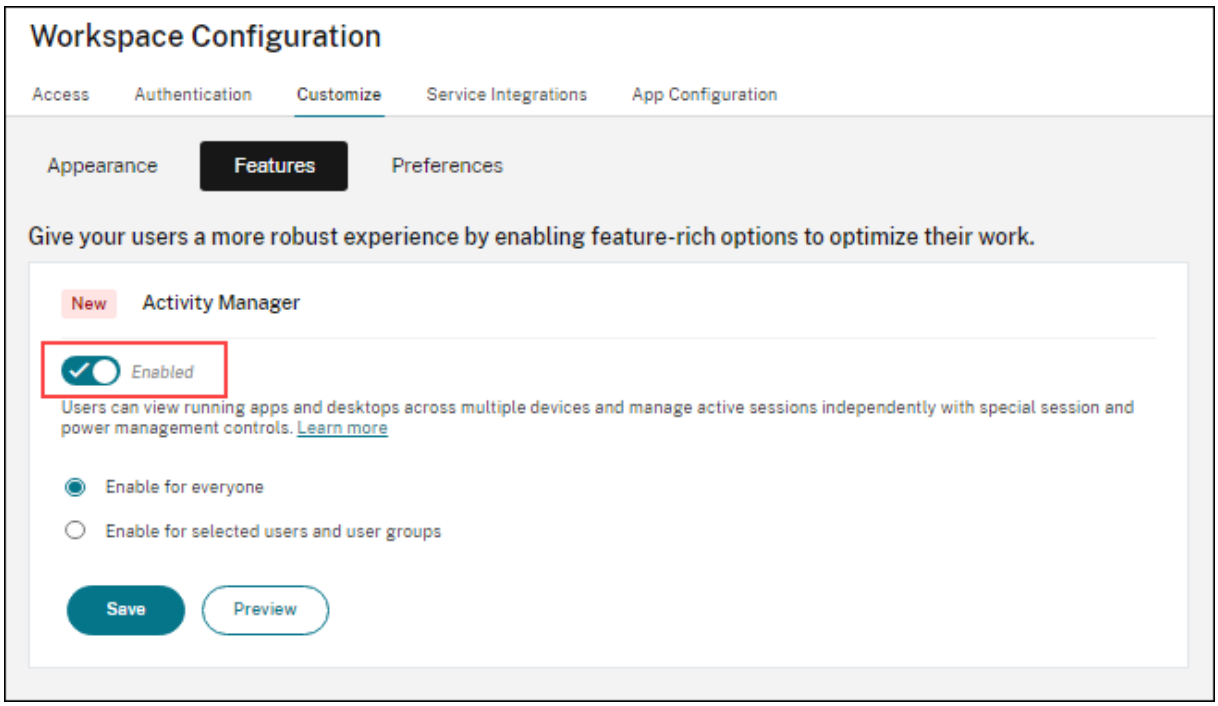



## Enable features for users

June 22, 2026

Use the Features tab to enable and disable features for your users.

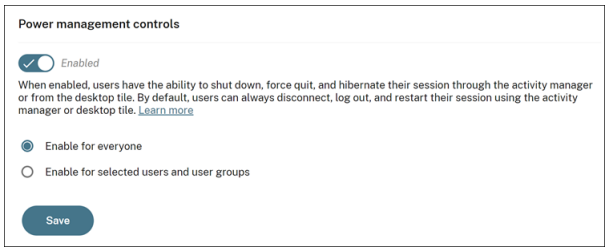



Currently the only configurable feature is Activity Manager power management.

### Power management controls

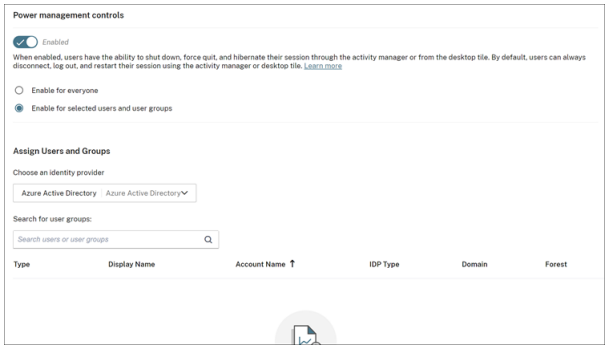
Power management controls include **Shut down**, **Force shutdown**, and **Hibernate**. To enable the power management control using Citrix Cloud™, do the following:

1. Navigate to **StoreFront Cloud** > **Customize** > **Features**.
2. Enable the toggle button.
3. Select **Enable for everyone** to apply the setting to all users.




4. Alternatively, select **Enable for selected users and user groups** to apply the setting to selected users and user groups.



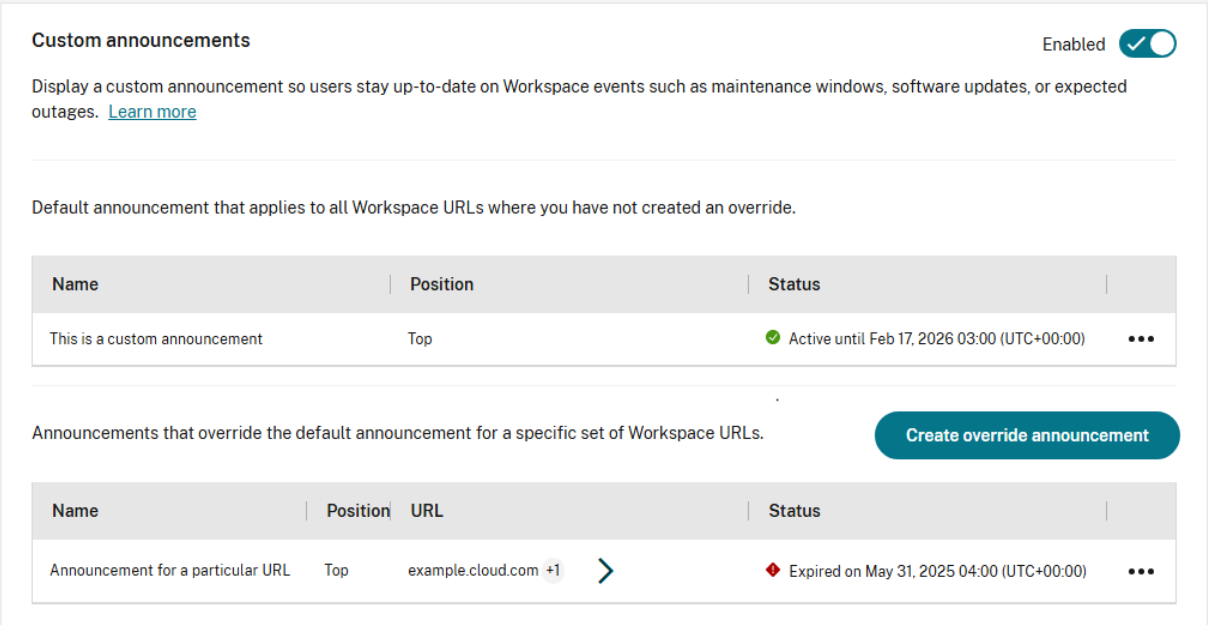

5. Click the down arrow and then choose an identity provider from the dropdown list.
6. In the **Search for user groups** text field, find users or groups to assign to this feature.

   Once you add the users or user groups, you can see their lists displayed on the screen.
7. Click **Save**.

## Custom announcements

June 22, 2026

You can send a custom announcement to your users during a given time period, for instance to inform them of an upcoming maintenance window. You can configure a default announcement along with an override for each store. Only a single announcement can be configured per store.




1. From the **Citrix Cloud** menu, choose **StoreFront Cloud**.

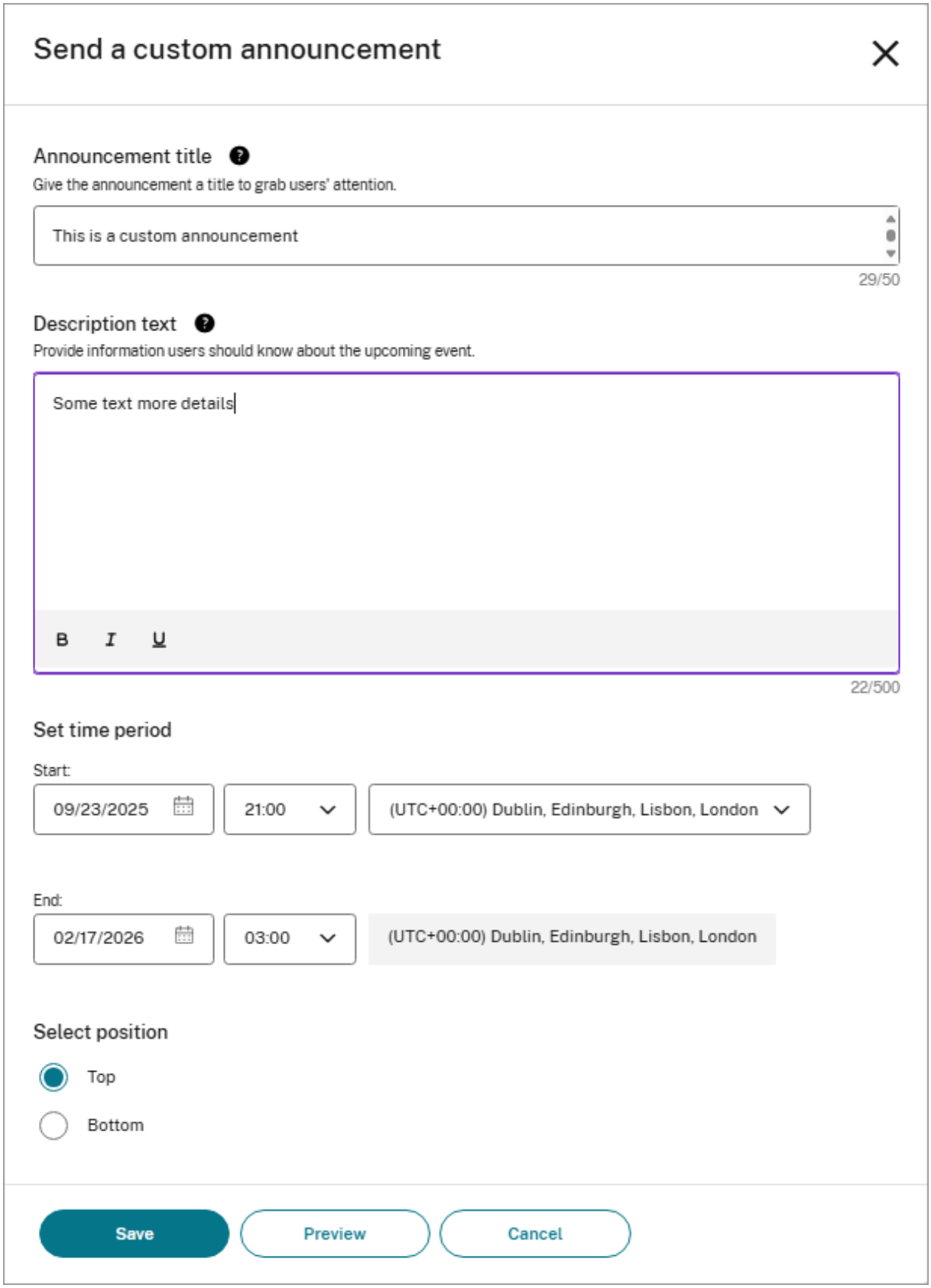
 

2. From the **Customize** menu, choose **Preferences**.
3. Go to the **Custom announcements** section.

### Create announcement

1. To add an announcement that applies to stores where there is no active override, select **Create default announcement**. To add an announcement for a specific store, select **Create override announcement**.
2. If you added an override announcement, choose which stores it applies to. This is not applicable to the default announcement.
3. Enter the **Announcement title**.
4. Enter the **Description text**.
5. Enter the time period during which the announcement should appear.
6. Choose whether to place the announcement at the top or bottom.
7. To view how your message appears to users, select **Preview**.
8. When you're finished, select **Save**.



### Delete announcement

1. In the row containing the announcement, select **...** to open the menu then select **Delete**.
2. In the confirmation window, select **Delete**.

### Edit announcement

1. In the row containing the announcement, select **...** to open the menu then select **Edit**.
2. Make changes as required.
3. Select **Save**.

## Allow end users to change their account password

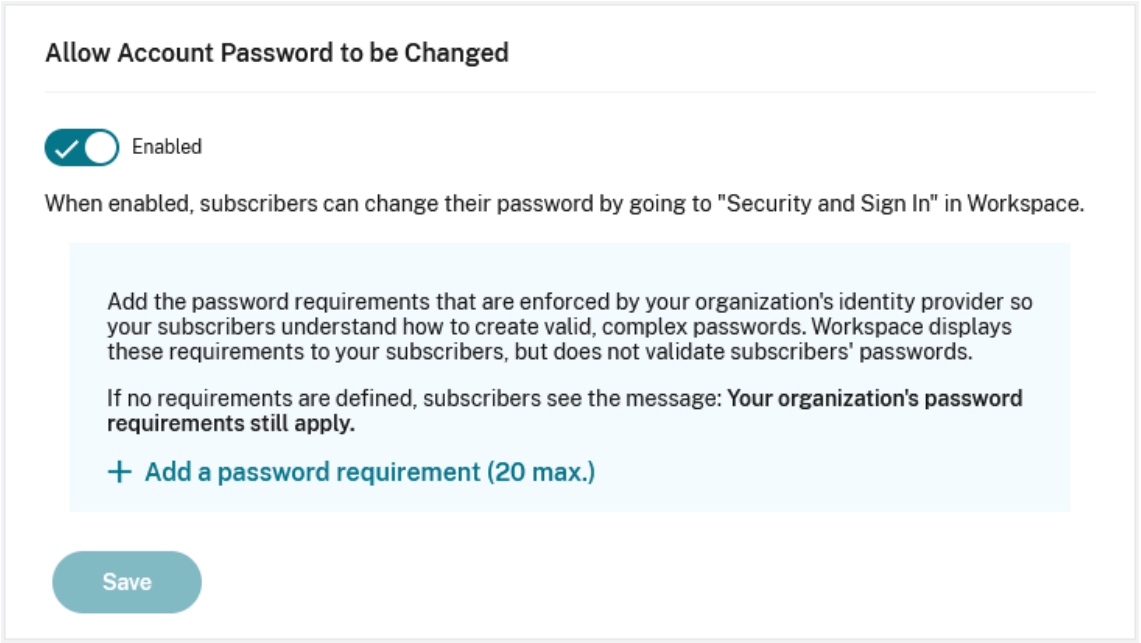
June 22, 2026

If you are using Active Directory or Active Directory (AD) plus token authentication then you can choose whether users can change their password. When enabled (default), users can change their password at any time, based on your organization's Active Directory settings. If disabled, store prompts end users to change their password when it expires, but they can't change their unexpired password at other times. To configure this:

Use the store Session settings to choose when users need to enter their credentials and for how long users remain logged in. To configure these settings:

1. From the **Citrix Cloud** menu, choose **StoreFront Cloud**.
2. From the **Customize** menu, choose **Preferences**.
3. Go to section **Allow Account Password to be Changed**.
4. Toggle **Enabled**.



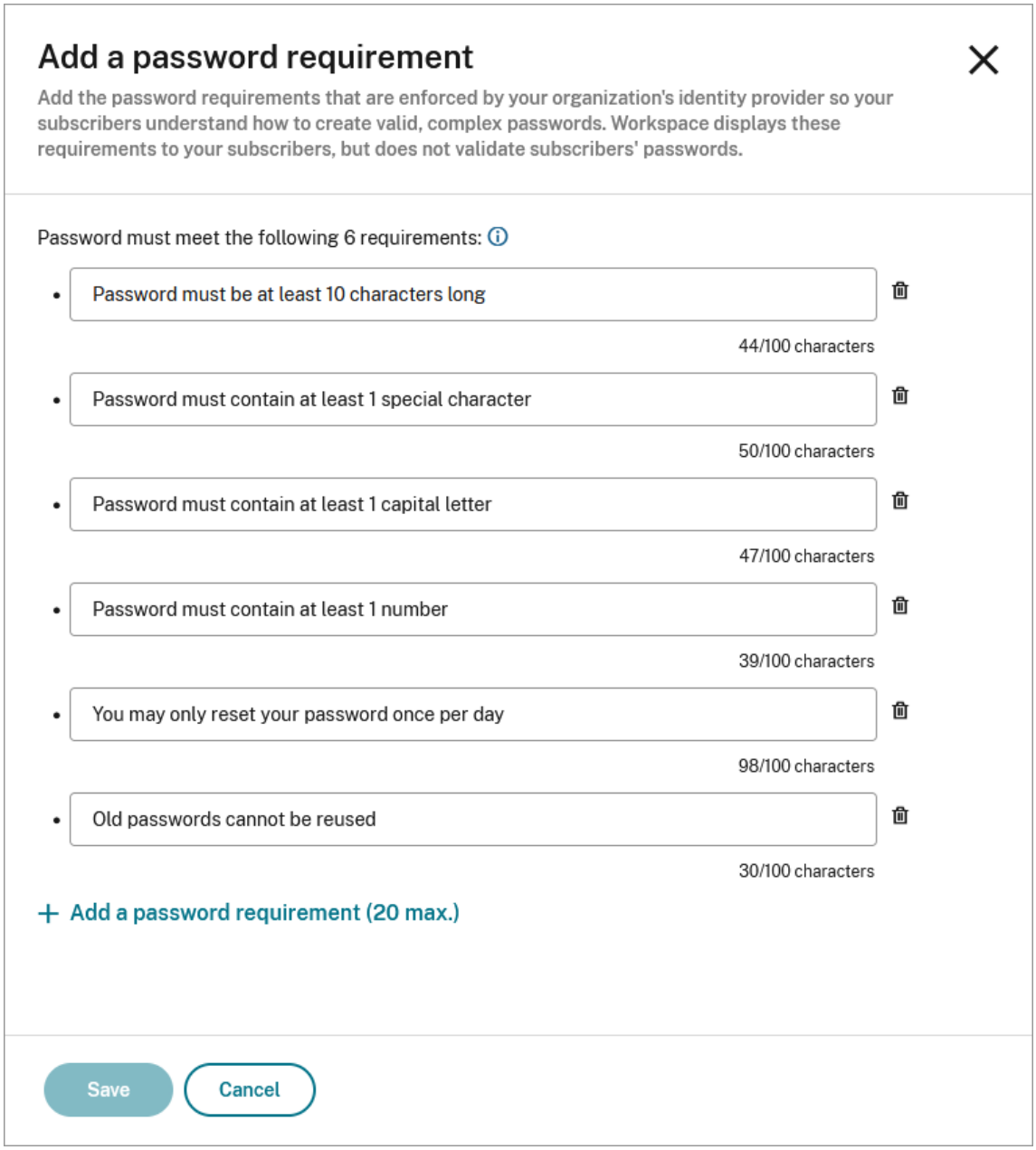

5. Press **Save** to save any changes.

You can add up to 20 password requirements to meet your organization's security policy and that your identity provider enforces. The store displays these requirements as a guide when end users change their password from their **Account Settings** page in the store end user interface. If you don't add any password requirements, the store displays the message "Your organization's password requirements still apply."

To add password requirements:

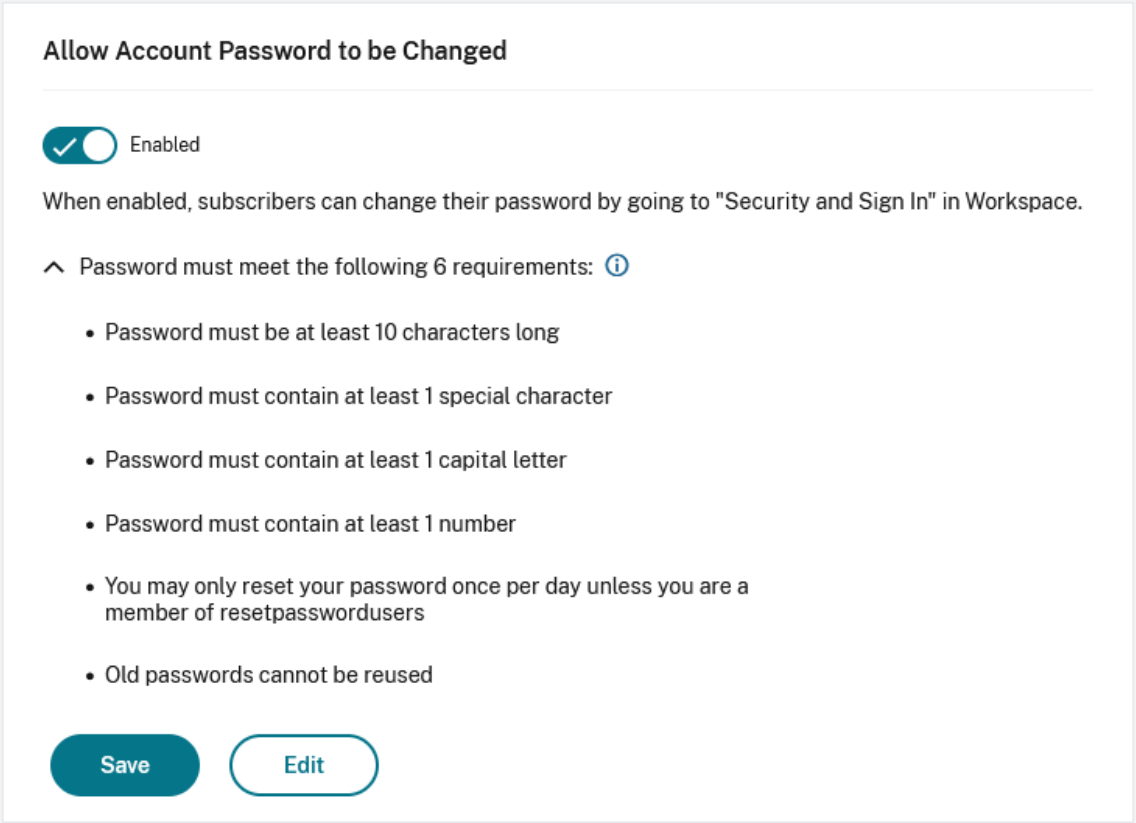
1. If there are currently no password requirements, select **Add password requirement**. If there is already at least one password requirement then select **Edit**.
2. Enter a requirement that matches your organization's security requirements for valid passwords. For example, you can specify that a password must be a certain character length. Select **Add a password requirement** to add more items for end users when they change their password.




3. When you're finished adding requirements, select **Save**. You can expand the list of requirements:




4. Select **Save** again to save all your setting changes.

## Supported clients

The following versions of Citrix Workspace app support this feature:

- Citrix Workspace app for Windows 2101 or later
- Citrix Workspace app for Mac 2012 or later
- Citrix Workspace app for Chrome 2010 or later
- Citrix Workspace app for Android 21.1.0 or later

End users can also use this feature when accessing stores from a web browser.

This feature isn't supported on the following:

- Older versions of Citrix Workspace app
- Citrix Workspace app for Linux

### End user experience when changing passwords

For more information, see Security & Sign in.

# Pinned links

June 22, 2026

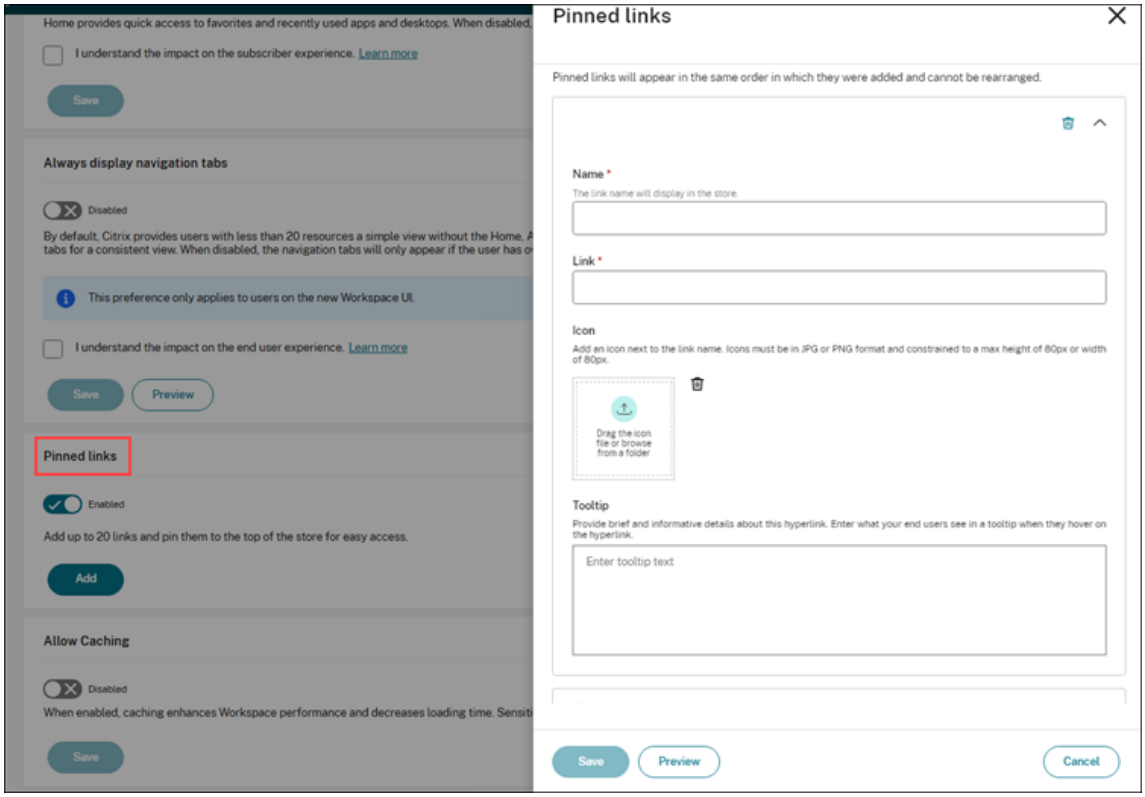
Pinned links are customer-defined hyperlinks that link to specific websites. Administrators can set up pinned links according to their preferences on store UI. This feature helps users to easily access specific websites simply by clicking the pinned links defined by the administrators. The pinned link requires a display name and a website URL. It can also be personalized with an icon and description, where the description provides brief information about the link.

## Configuration

Administrators can manage this feature on user devices using their Citrix Cloud account.

To enable this feature, follow these steps:

1. Navigate to **StoreFront Cloud** > **Customize** > **Preferences** in the Citrix Cloud account.
2. Under **Pinned links**, toggle the button to enable the feature. A new window appears.




3. In the **Name** text field, enter the name of the link that you want to pin on the store UI.
4. In the **Link** text field, enter the URL of the website.

5. Under **Icon**, attach an icon if you want to display it next to the pinned link.
6. Under **Tooltip**, provide a brief description about the website, which appears when users hover their mouse over the pinned link.
7. Click **Preview** if you want to preview the changes. This action is optional.
8. Click **Save** to save your changes.

> **Note:**
>
> The fields marked with an asterisk are mandatory.

## User interface settings

June 22, 2026

To modify user interface settings:

1. From the **Citrix Cloud** menu, choose **StoreFront Cloud**.
2. From the **Customize** menu, choose **Preferences**.
3. Go to the appropriate section:
    - Allow caching
    - Allow favorites
    - Navigation tabs

### Allow Caching

The **Allow Caching** setting enhances performance for end users accessing their store through a web browser. This option does not apply when using a locally installed Citrix Workspace app.

When caching is enabled, some sensitive data might be stored locally on end users'devices. This data consists of file metadata and is encrypted with a key that's unique to the end user's authenticated identity. The encrypted data is stored on the user's device in the web browser's local storage.

If you disable caching, the encrypted data is purged the next time the end user signs in to a store through their web browser. Also, the user can purge this data manually by clearing browsing data from their web browser.

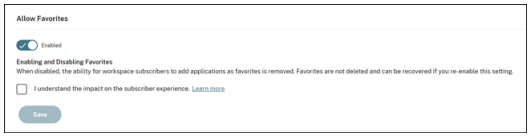
 

## Allow Favorites

Customers, who have access to **StoreFront Cloud** and the new store experience, can allow users to add or remove their favorite apps and desktops on Citrix Workspace app. Users can quickly access their favorite apps and desktop on the **Home** tab. The **Allow Favorites** feature is enabled by default.

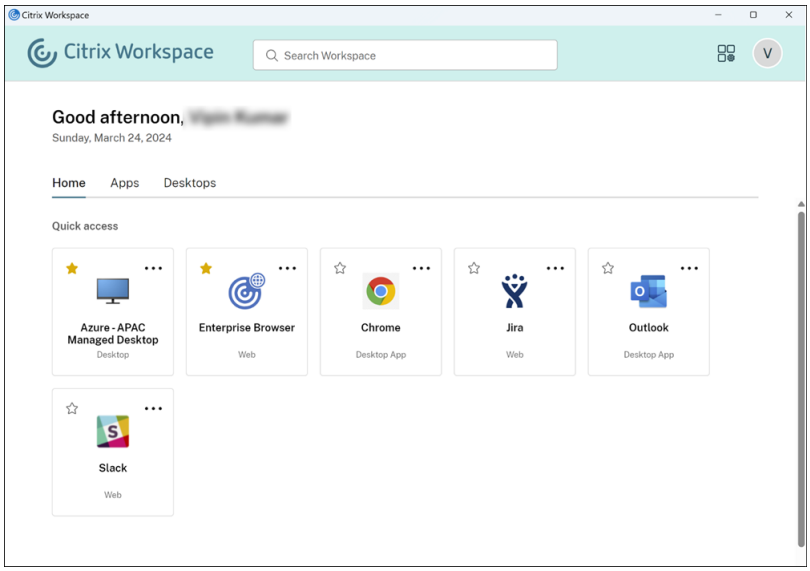
To configure the **Allow Favorites** feature, do the following instructions:

1. Navigate to **StoreFront Cloud** > **Customize** > **Preferences**.
2. Click the toggle button to enable or disable the feature.
3. Select the declaration check box, and click **Save**.




### User experience

When you enable the **Allow Favorites** feature, users can add up to 250 favorites by clicking the star icon at the upper-left corner of apps and desktops cards. The star icon turns to a golden color when users mark it as their favorite. Clicking the star icon again removes it from the favorite list.




When a user adds more than 250 favorite resources, the oldest favorite resource is removed (or as close as possible) to preserve the most recent favorite resources.

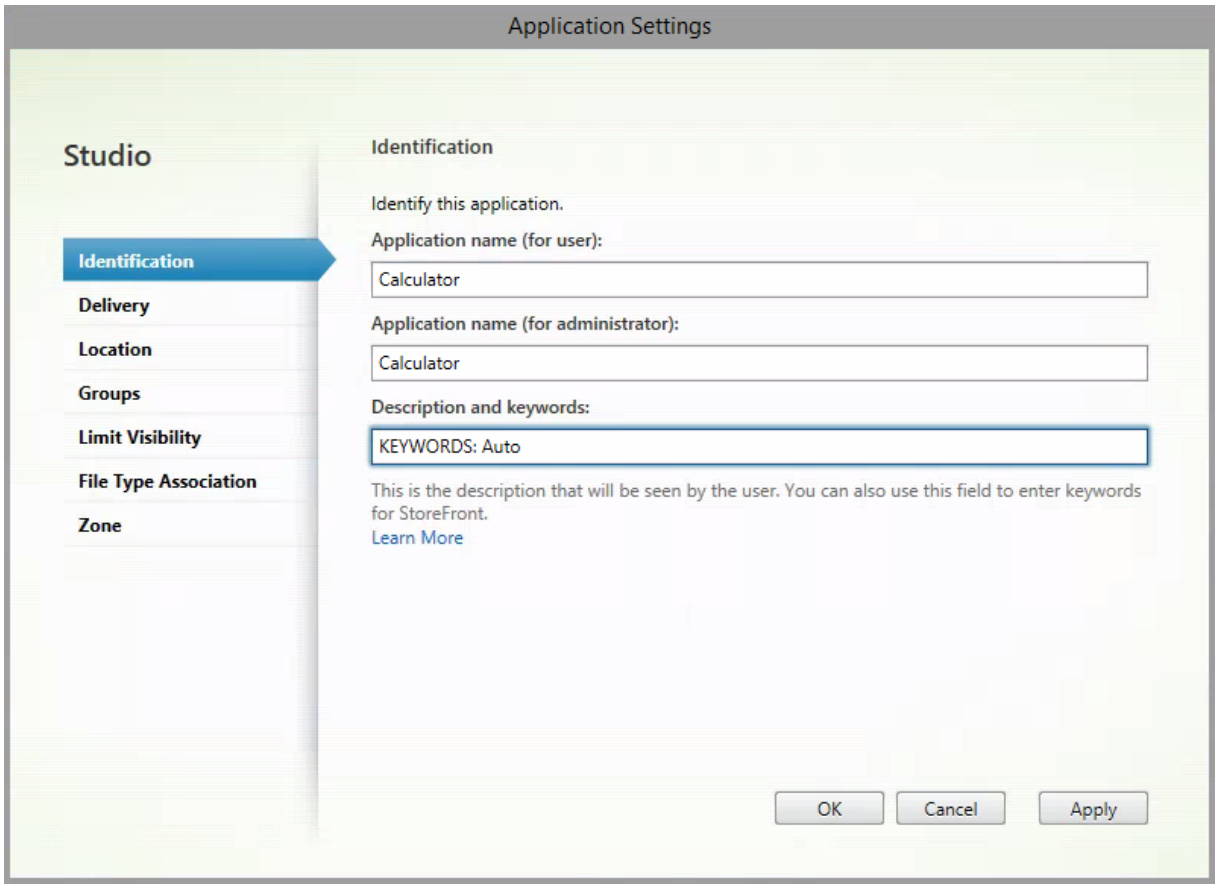
When you disable the **Allow Favorites** feature, the favorites resources get removed from the **Home** tab of Citrix Workspace app. And, it's not available for quick access. Users can still access those resources from the **Apps** tab and **Desktops** tab.

> **Note:**
>
> - **Allow Favorites** feature is enabled by default.
> - If your users don't have access to the desktops configured, the **Desktop** tab doesn't appear on the navigation bar.

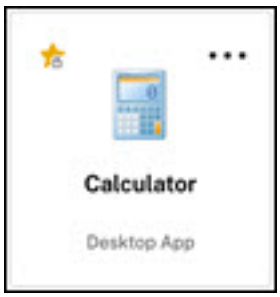
### Apps and Desktops keywords

You can automatically add favorite apps or desktops for users by using `KEYWORDS:Auto` and `KEYWORDS:Mandatory` settings in Citrix DaaS (**Manage** > **Full Configuration** > **Applications**).




- **KEYWORDS:Auto** - The app or desktop is added as a favorite and users can remove it from the favorite list as per their preference.
- **KEYWORDS:Mandatory** - The app or desktop is added as a favorite, and users can't reverse this action. Mandatory apps and desktops display a star icon with a padlock to indicate that it can't be removed from the favorite list.




> **Note:**
>
> If you use both **Mandatory** and **Auto** keywords for an app, the **Mandatory** keyword overrides the **Auto** keyword, and the apps or desktops that are added as favorites can't be removed.

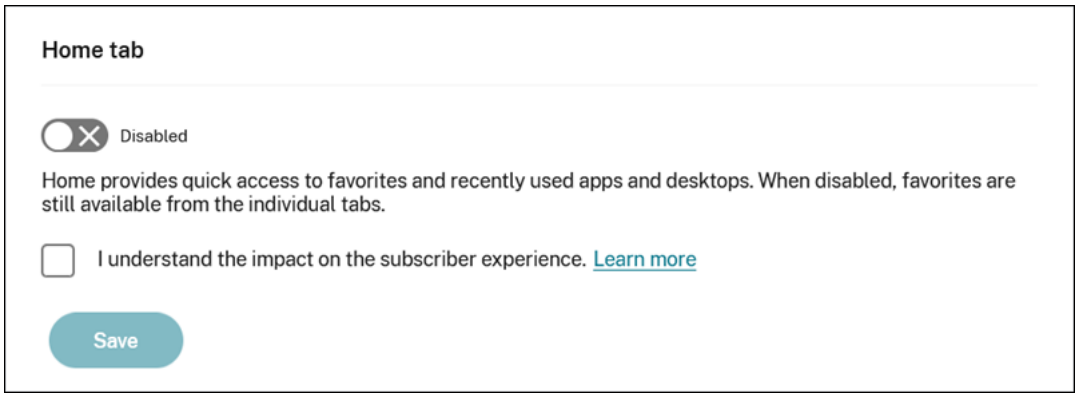
## Navigation tabs

### Home tab

You can enable or disable the **Home** tab for your users.

To configure the setting:

1. Under **Home tab**, set the toggle to **Enabled** or **Disabled**.
2. Select the declaration check box.
3. Click **Save**.
4. When the toggle is on, users are navigated to the **Home** page. If you disable the toggle, the users land directly on the **Apps** page. By default, the toggle is on and the feature is enabled.




When enabled (the default), the **Home** tab is displayed. When disabled, there is no **Home** tab and users land on the **Apps** tab.

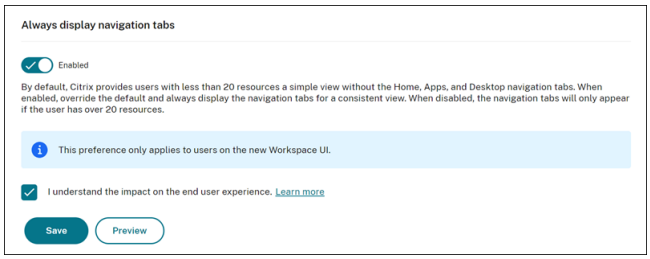
This feature does not apply when Always display navigation tabs is disabled and users have more than 20 apps or desktops. In this case, the tabs are hidden.

### Always display navigation tabs

By default, if the user has fewer than 20 resources, the UI displays a Simple View that doesn't have any tabs or categories. To disable the Simple View and enable the navigation tabs for a consistent experience, even if there are fewer than 20 resources, do the following:

1. For setting **Always display navigation tabs**, select the toggle to set it to **Enabled** or **Disabled**.
2. Click **Save**.



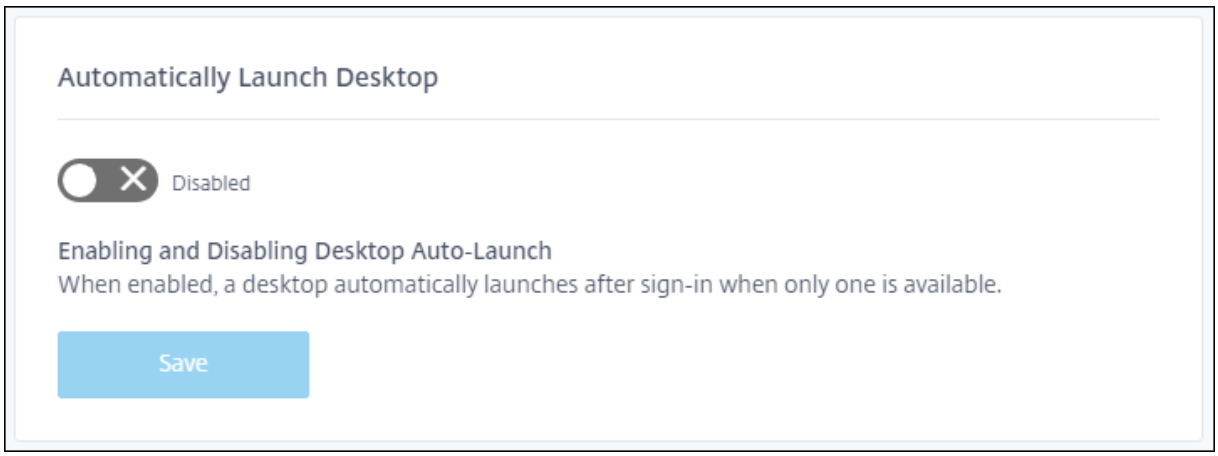

### Automatically Launch Desktop

You can configure store to automatically launch the user's desktop. When enabled, if a user has only one available desktop, the desktop automatically launches when the user signs in to their store. When disabled (default), users must manually launch their desktop after signing in.

This feature only applies when using a web browser, not Citrix Workspace app.

To change the configuration:

1. Navigate to **StoreFront Cloud** > **Customize** > **Preferences**.
2. Under **Automatically Launch Desktop**, set the toggle to **Enabled** or **Disabled**.
3. Press **Save**.



# Store Sessions

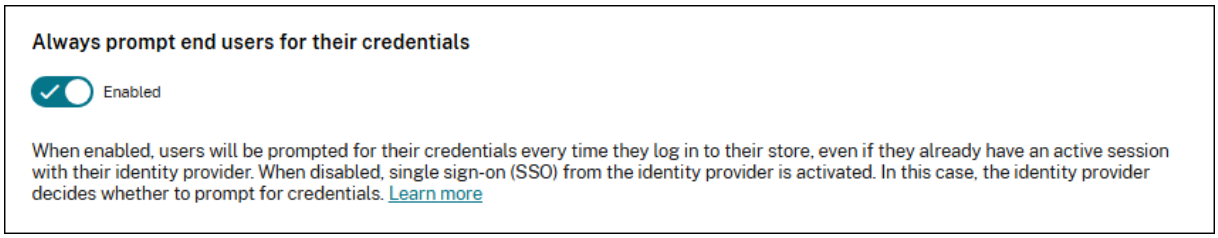
June 22, 2026

Use the store Session settings to choose when users need to enter their credentials and for how long users remain logged in. To configure these settings:

1. From the **Citrix Cloud** menu, choose **StoreFront Cloud**.
2. From the **Customize** menu, choose **Preferences**.
3. Go to the **store Sessions** section.
4. Update the settings.
5. Press **Save** to apply them or **Revert** to cancel them.

Some settings can be configured differently according to the network location connectivity type. This requires using PowerShell modules. For more information, see Configure settings per network connectivity type.

## Always prompt end users for their credentials



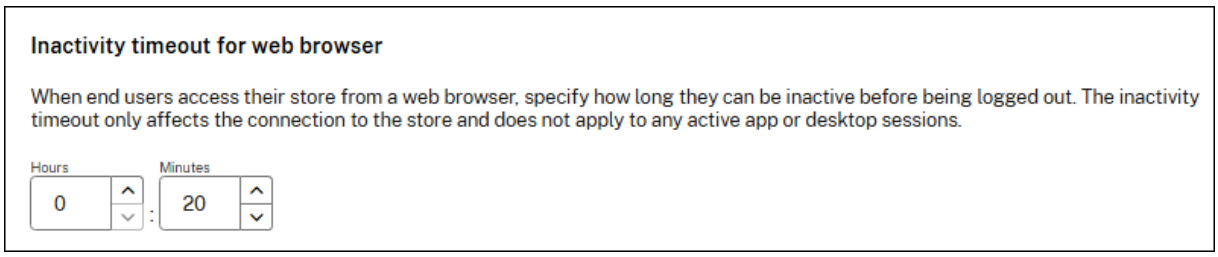

When enabled (default), store forces a sign-in prompt with the identity provider when a new store session is needed. For OIDC authentication, store includes `prompt=login` in the authentication request. For SAML authentication, store sends `ForceAuthn=true` in the authentication request.

When disabled, users might not be prompted to authenticate with the identity provider if the identity provider already has a valid session.

## Inactivity timeout for web browser

Use the **Inactivity timeout for web browser** setting to specify the amount of idle time allowed (a maximum of 8 hours) before users are automatically logged out. Only interactions with store, such as refreshing the page or launching an app, count as activity.




Unlike manual sign-out, which disconnects DaaS sessions, users stay connected to their DaaS sessions even after timeout due to inactivity. The users are not signed out from their Identity Provider. Therefore if **Always prompt end users for their credentials** is off, the user might be able to log back in without entering their credentials.

See also Configuring settings per network connectivity type.

### Inactivity timeout for Citrix Workspace app

#### Desktop

Use the **Desktop** option of **Inactivity timeout for Workspace app** setting to specify the amount of idle time allowed (a maximum of 24 hours) before users are automatically signed out of Citrix Workspace app for Windows, Mac and Linux. Any interaction with the mouse or keyboard counts as activity and extends the timeout.

Unlike manual sign-out, which disconnects DaaS sessions, end users stay connected to their DaaS sessions even after timeout due to inactivity.

You can modify the setting using the PowerShell module. Use the `Set-WorkspaceCustomConfiguration` cmdlet with parameter `InactivityTimeoutInMinutes`.

See also Configure settings per network connectivity type.

#### Mobile

Use the **Mobile** option of **Inactivity timeout for Workspace app** setting to specify the amount of idle time allowed (a maximum of 24 hours) before Citrix Workspace app is locked. This applies to Citrix Workspace app for iOS and Android. Once locked, users must use biometrics or their device PIN to unlock Citrix Workspace app. If biometrics is not enabled on the device then the user is instead logged out.

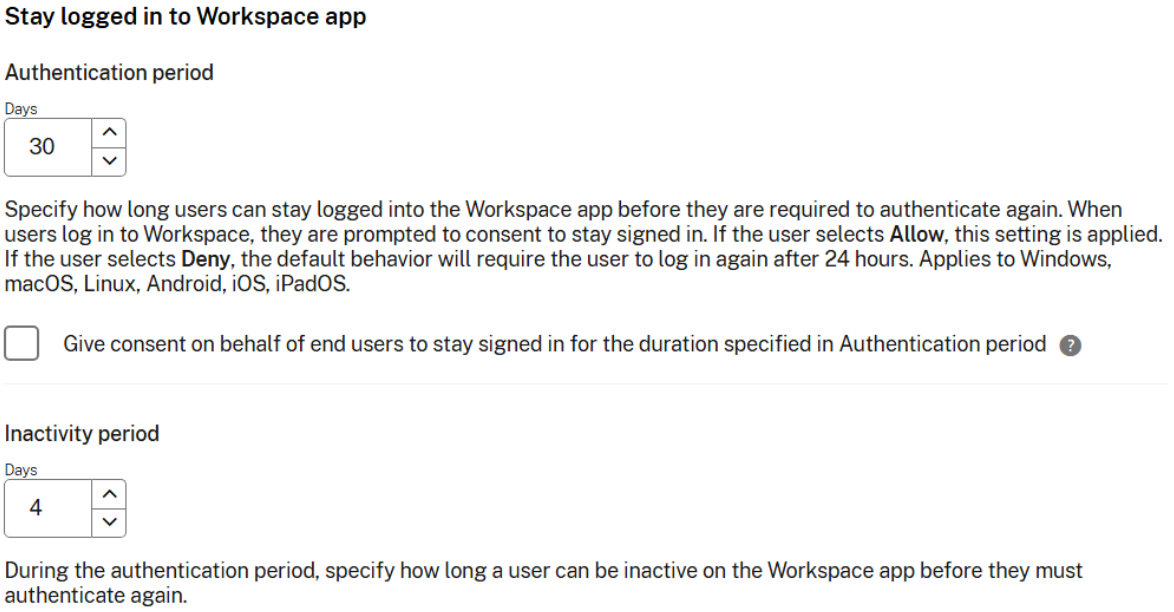
You can modify the setting using the PowerShell module. Use the `Set-WorkspaceCustomConfiguration` cmdlet with parameter `InactivityTimeoutInMinutesMobile`.

See also Configure settings per network connectivity type.

### Stay logged in to Citrix Workspace app

Use the **Stay logged in to Workspace app** settings to specify the length of time users can stay signed in to Citrix Workspace app before needing to sign in again. These settings do not apply to web browsers.




The **Authentication period** defines the maximum time before users must reauthenticate. By default this is set to 30 days but you can configure a value between 1 and 365 days.

If the period is greater then 1 day then by default when a user authenticates they are prompted for consent to "Stay signed in", see user experience. This allows the Citrix Workspace app to use a refresh token to obtain new access tokens when the existing ones expire. The user must accept the permission to continue. If the user rejects the permission then they are returned to the log in screen. If the user enters their credentials a second time then they are not shown the prompt and their session is limited to 24 hours.

If you select **Give consent on behalf of end users to stay signed in for the duration specified in Authentication period**, this removes the need for users to individually provide consent to stay signed in.

The **Inactivity period** defines how long a user can be inactive before they must reauthenticate. By default this is 4 days but you can configure it to a value between 1 day and the Reauthenticaiton Period. If a user is inactive for more than this value, they are prompted to reauthenticate the next time that they attempt to access their store. To set an inactivity period of less than 24 hours on desktop, use the **Desktop** option of Inactivity timeout for Citrix Workspace app setting.

#### Revoking permission to stay signed in

You can invalidate the session for your end users by downloading this PowerShell script and following the instructions included in the download. Once you've invalidated sessions, users must reauthenticate to their stores in the next 24 hours.

#### Supported Workspace app clients

The following versions of Citrix Workspace app support this feature:

- Workspace app 2106 for Windows or later
- Workspace app 2106 for Mac or later
- Workspace app for 21.6.5 iOS or later
- Workspace app for 21.6.0 Android or later

#### Supported authentication methods

Staying signed in to Citrix Workspace app is supported for the following authentication methods:

- Active Directory
- Active Directory plus token
- Entra ID
- Citrix Gateway
- Okta

> **Note:**
>
> For the same experience as a Citrix DaaS customer using Okta or Azure Active Directory, configure the Citrix Federated Authentication Service (FAS). For more information about FAS, see Enable single sign-on for stores with Citrix Federated Authentication Service.

### Configure settings per network connectivity type

You can configure the web, desktop and mobile timeouts, along with **Always prompt end users for their credentials**, differently according to whether the user is on your internal network, a known external network or anywhere else. For instance you could configure shorter timeouts for devices connected to your internal network.

#### View existing configuration

To view existing configuration using the Citrix® StoreFront Cloud PowerShell module, call `Get-StoreClientLocationConfiguration` cmdlet. For example:

```
$ConnectivityTimeouts = Get-StoreClientLocationConfiguration -StoreUrl
    "https://customer.cloud.com" `
                                                                -ClientId
                                                                    '
                                                                    myclientid
                                                                    ' `
                                                                -
                                                                    ClientSecret
                                                                     '
                                                                    mysecret
                                                                    '
$ConnectivityTimeouts.external
$ConnectivityTimeouts.internal
$ConnectivityTimeouts.undefined
```

### Update configuration

To configure the setting for a network connectivity type:

1. Ensure that Adaptive Access is enabled.
2. Define Network locations representing your internal locations and external known locations, based on the user's public IP address. If the user's IP address does not match a network location then its network connectivity type is considered to be undefined.
3. From the Citrix® StoreFront Cloud PowerShell module, call `Set-StoreClientLocationConfigurati` cmdlet with the `Internal`, `External` or `Undefined` parameters. The parameter value must be a hashtable with keys `inactivityTimeoutInMinutesWeb`, `inactivityTimeoutInMinut` , `inactivityTimeoutInMinutesMobile` and `promptLoginEnabled`.

For example to so set overrides for each location, run:

```
$InternalHashTable = @{
 promptLoginEnabled=$false;
                      inactivityTimeoutInMinutesWeb='60';
                      inactivityTimeoutInMinutesDesktop='60';
                      inactivityTimeoutInMinutesMobile='120' }

$ExternalHashTable = @{
 promptLoginEnabled=$true;
                      inactivityTimeoutInMinutesWeb='60';
                      inactivityTimeoutInMinutesDesktop='60';
                      inactivityTimeoutInMinutesMobile='120' }

$UndefinedHashTable = @{
 promptLoginEnabled=$true;
                      inactivityTimeoutInMinutesWeb='20';
                      inactivityTimeoutInMinutesDesktop='20';
                      inactivityTimeoutInMinutesMobile='20' }

```

```
19
20 Set-StoreClientLocationConfiguration -StoreUrl "https://customer.cloud.
       com" `
21                                        -ClientId 'myclientid' `
22                                        -ClientSecret 'mysecret' `
23                                        -Internal $InternalHashTable `
24                                        -External $ExternalHashTable `
25                                        -Undefined $UndefinedHashTable
```

If you do not configure a specific timeout for the network connectivity type then the non-location-specific timeout is used instead.

To remove overrides, set the Internal, External or Undefined parameter to null. For example:

```
1 Set-StoreClientLocationConfiguration -StoreUrl "https://customer.cloud.
      com" `
2                                        -ClientId 'myclientid' `
3                                        -ClientSecret 'mysecret' `
4                                        -Internal $NULL `
5                                        -External $NULL `
6                                        -Undefined $NULL
```

> **Important:**
>
> If the user device moves to a network with a different connectivity type then the new values do not apply immediately. Citrix Workspace app updates the values every 90 minutes. If using a web browser, the values update the next time the user refreshes the web page.

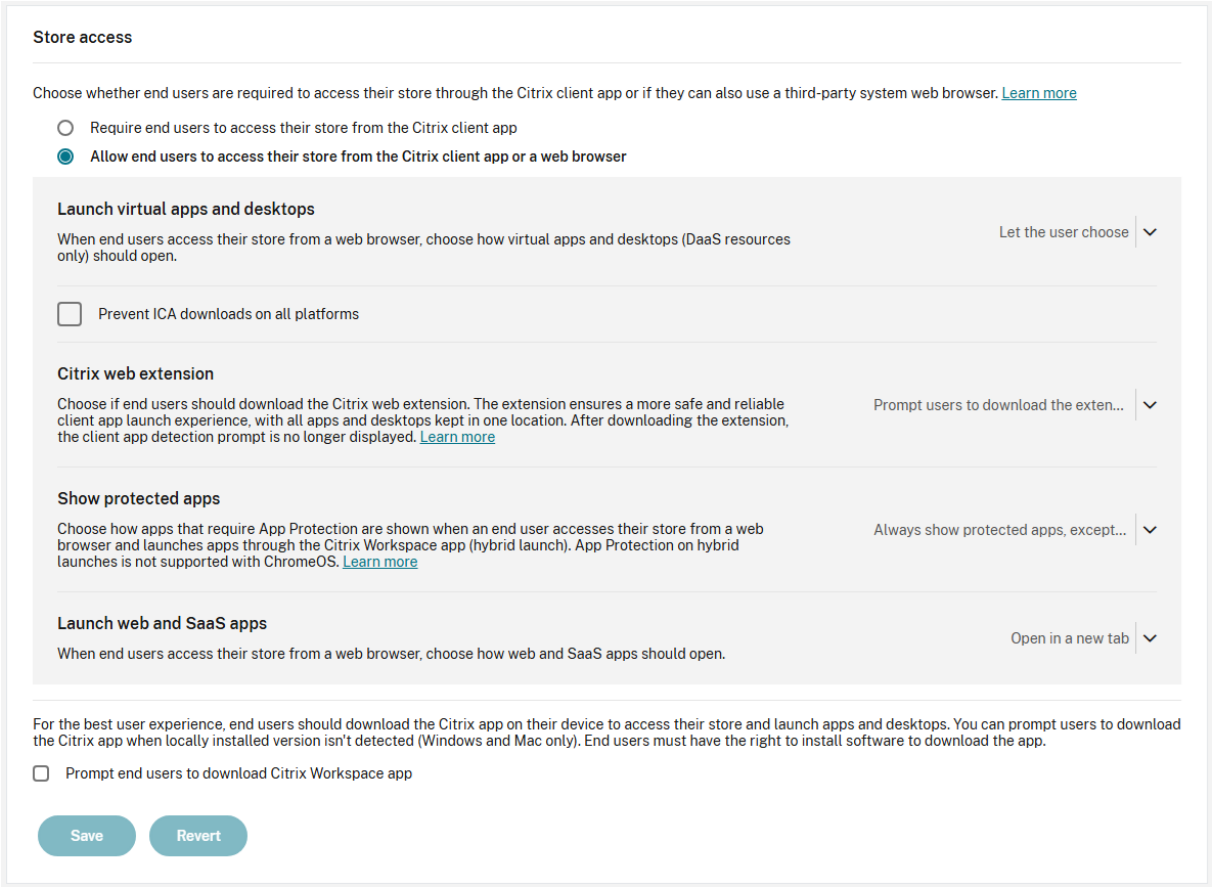
## Store access

June 22, 2026

In Store access settings you can configure the following:

- Whether users are required to open their store in Citrix Workspace™ app or whether they can use a web browser.
- When opening their store in a web browser, whether virtual apps and desktops always open in a browser or Citrix workspace app.
- When opening their store in a web browser, whether they must install Citrix® Web extension.




To configure store access settings:

1. Log in to Citrix Cloud console.
2. From the **Citrix Cloud** menu, choose **StoreFront Cloud**.
3. From the **Customize** menu, choose **Preferences**.
4. Go to the **Store access** section.
5. Update the setting as required.
6. Select **Save** to save your changes.

### Require Citrix Workspace app

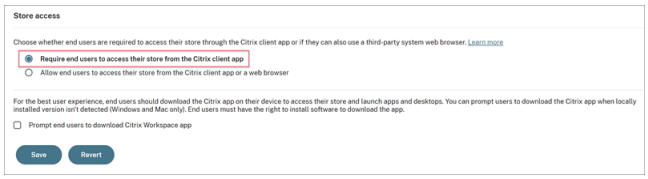
Enforcing native Citrix Workspace app on user devices implies restricting end users to sign in and use only the locally installed Citrix Workspace app. By doing so, end users can't access their store using a web browser. This feature is designed for customers who want to use the full benefits of Citrix Workspace app.

### Configuration

Administrators can use their Citrix Cloud account to mandate the use of native Citrix Workspace app on user devices. To manage this feature, follow these steps:

1. Select **Require end users to access their store from the Citrix client app**.




   [Optional] Select **Prompt end users to download Citrix Workspace app** to prompt the users to download Citrix Workspace app if they don't have the app installed on their device. For more information, see Configure native app download link for end users.

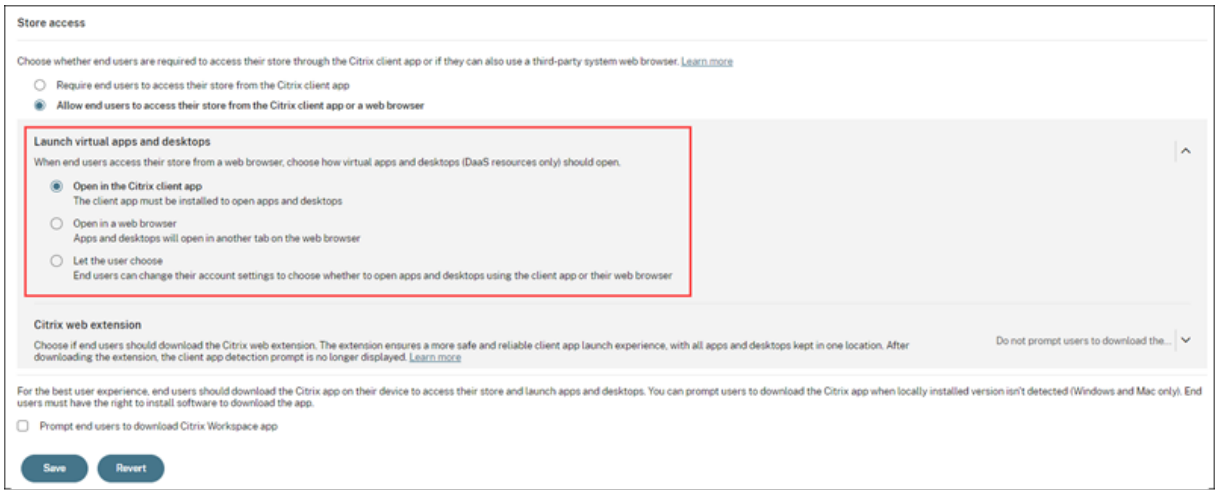
2. Click **Save** to save the changes, or click **Revert** to discard the changes.

### End user experience

For details on the user experience, see Require Citrix Workspace app.

## Launch virtual apps and desktops

If you have allowed users to open the store in their web browser then you can then choose whether applications are also launched within the web browser or in Citrix Workspace app.




Choose one of the following settings:

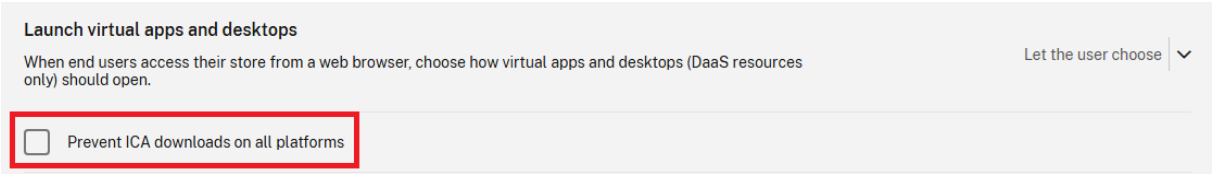
- **In the Citrix client app** (default): End users are required to use a locally installed version of the Workspace app.

- **In a browser** End users are required to launch virtual apps and desktops in their web browser. Choose this option if users are not able to install software locally.
- **Let the user choose:** When users first open the store in their browser, they can choose whether to launch virtual apps and desktops in Citrix Workspace app or their browser.

### Prevent ICA downloads

If you have allowed users to open the store in their web browser and launch in Citrix Workspace app then you can configure the store to prevent ICA downloads.




When this setting is enabled, the Citrix Workspace app detection does not display the option to **Skip detection**. Users must either install Citrix web extension or successfully complete detection using Citrix Workspace Launcher.

> **Important:**
>
> This setting prevents launching resources if Citrix Workspace launcher and Citrix web extensions are not available, including on ChromeOS. For a list of supported browsers and clients, see Citrix Workspace launcher and Citrix web extensions.

#### Prevent ICA downloads using PowerShell

You can use the PowerShell API cmdlet `Set-StoreConfigurations` with the following parameters.

`-AllowSkipNativeAppDetection` - Configures whether users have the option on the Citrix Workspace app detection screen to **Skip detection**.

`-PreventIcaDownloads` - Configures whether all ICA file downloads are blocked, including on platforms that do not support Citrix Workspace launcher. If `-AllowSkipNativeAppDetection` is enabled then ensure `-PreventIcaDownloads` is disabled.

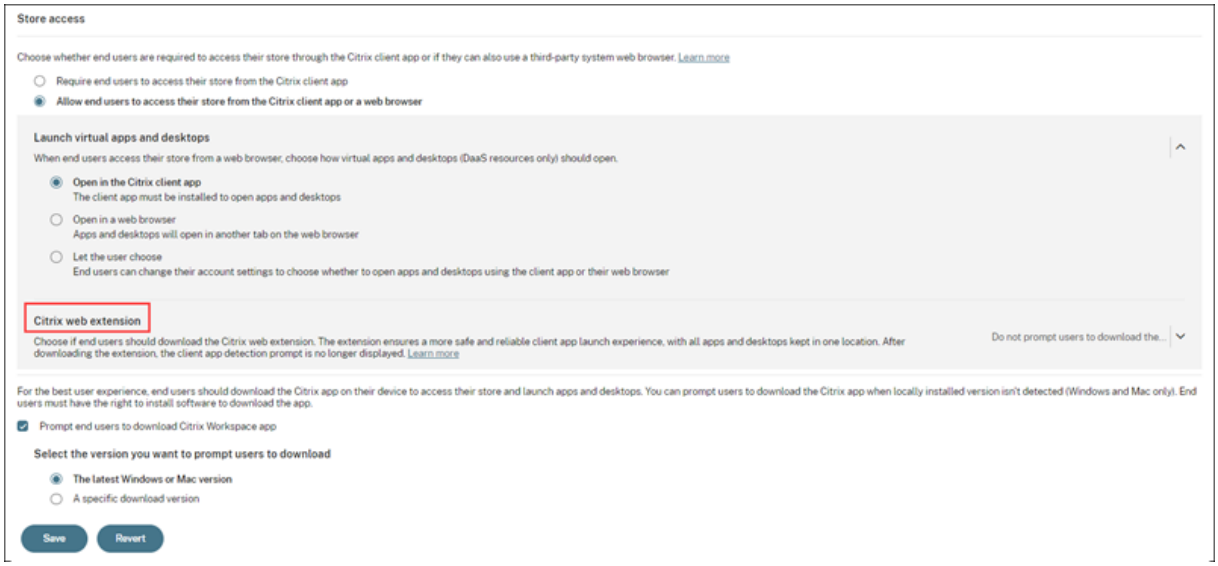
The deprecated setting `-DisallowICADownload` corresponds to the inverse of `-AllowSkipNativeAppDet`
.

### Manage installation prompt for Citrix web extension

If you have allowed users to access their store from a web browser, you can configure whether the website prompts the user to install Citrix Web Extension. The prompt only appears if the website does

not detect the extension.




Set **Citrix web extension** to one of the following values:

- **Prompt end users to download the Web Extension but allow access to the store if it isn't detected** (default): The website prompts the end user to install the extension. They are allowed to use store even if they decide to install the store Web Extension later.
- **Require end users to download the Citrix Web Extension and block access to the store until it is detected:** End users aren't allowed to use store until they install the store Web Extension.
- **Do not prompt end users to download the Citrix Web Extension:** The store doesn't prompt end users to install Citrix web extension.

### Show or hide resources requiring App Protection

App protection provides additional security against screen capture and key logging.

When users open their store in a version of Citrix Workspace app that supports App Protection, the app always displays resources requiring App Protection. Legacy versions of Citrix Workspace app hide resources requiring App Protection. For supported versions, see System requirements.

When users open their store in a web browser and launch resources in Citrix Workspace app, you can configure whether the user interface displays resources requiring App Protection. You can choose from the following options.

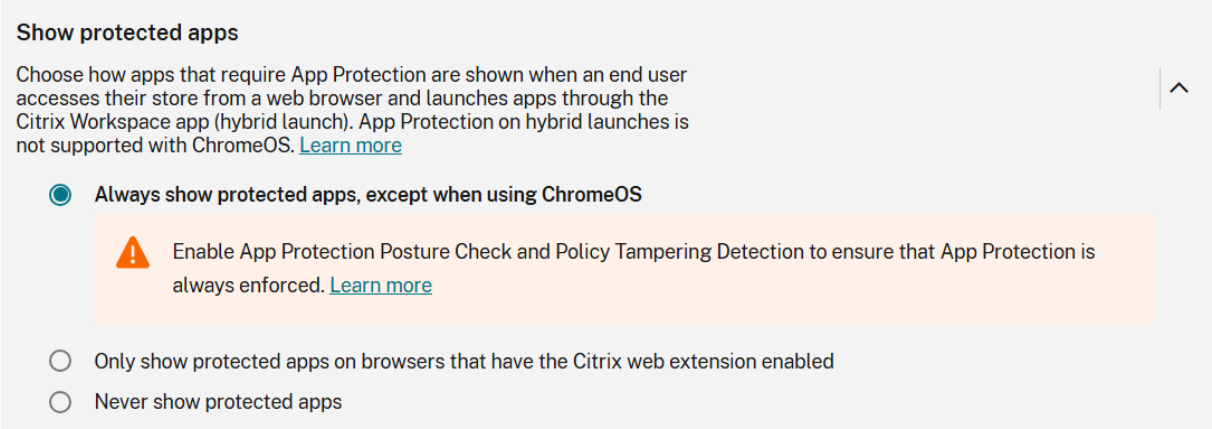
- **Always show protected apps, except when using ChromeOS**. New deployments of Citrix® StoreFront Cloud use this as the default. In some cases, the store is not aware of which version of Citrix Workspace app is installed, so may display resources when users use a legacy client that is not capable of applying App Protection. Therefore Citrix recommends that you enable App protection posture check to validate the client capability when starting the session. If users can

download ICA files, then they can modify the ICA file before launching the resource. Therefore Citrix recommends that you enable App protection tampering detection.

- **Only show protected apps on browsers that have Citrix web extension installed**. Older deployments of Citrix® StoreFront Cloud used this as the default. Citrix web extension provides additional security by checking the version of Citrix Workspace app and transfers the ICA file in-memory to prevent tampering. If the user has not installed Citrix web extension, the store hides all resources requiring App Protection.
- **Never show protected apps**. With this option, the store does not display resources requiring App Protection, preventing them from being launched.

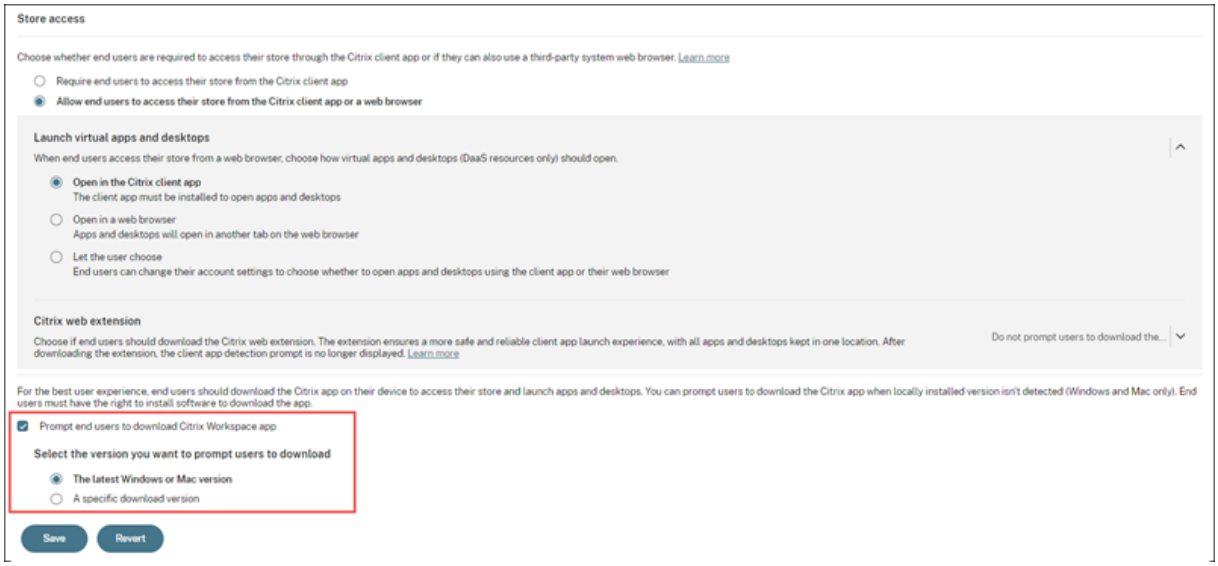
> **Note:**
>
> - Citrix Workspace app for Chrome OS cannot apply App Protection. Therefore on ChromeOS the store website always hides resources requiring App Protection.
> - The browser HDX client cannot apply App Protection. Therefore, if users choose to open resources in their web browser, the store website always hides resources requiring App Protection.




### Configure native app download link for end users

Administrators can prompt end users to download Citrix Workspace app if they don't have the app installed on their device.




Select either of the following option:

- **The latest Windows or Mac version:** Prompts users to download the latest version of Citrix Workspace app on their devices. When users click the download link, they're redirected to the respective download page.

> **Note:**
>
> For devices running Linux, when users click the download link, it opens the Citrix Download page where the users can manually download the executable file. For ChromeOS, Android and iOS devices, the download link redirects users to the Chrome Web Store, Play Store, and App Store respectively.

- **A specific download version:** In the **Download URL** text field, provide the URL of the Citrix Workspace app version you want users to download.

> **Note:**
>
> Administrators need to provide the download URL for the specific version of Citrix Workspace app based on the operating system of the user device. If there are users who have both Windows and Mac devices, administrators can give a common link that directs to Citrix Workspace app download page instead of giving a URL for just one operating system.

## Log in dialog

June 22, 2026

You can configure the store to display a message before or after the user logs in.

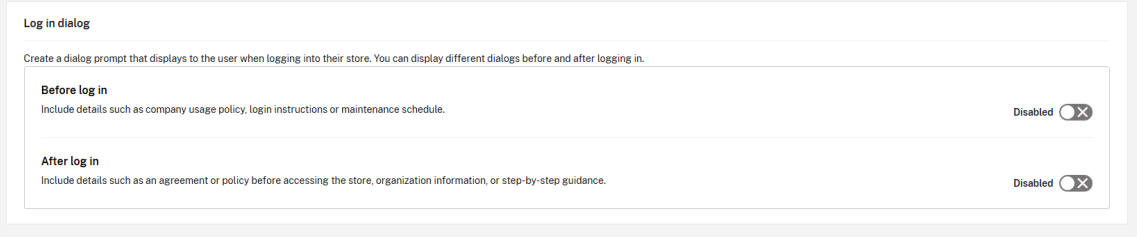
To configure log in dialogs:

1. Log in to Citrix Cloud™ console.
2. From the **Citrix Cloud** menu, choose **StoreFront Cloud**.
3. From the **Customize** menu, choose **Preferences**.
4. Go to the **Log in dialog** section.

### Configure a custom dialog to be displayed before log in

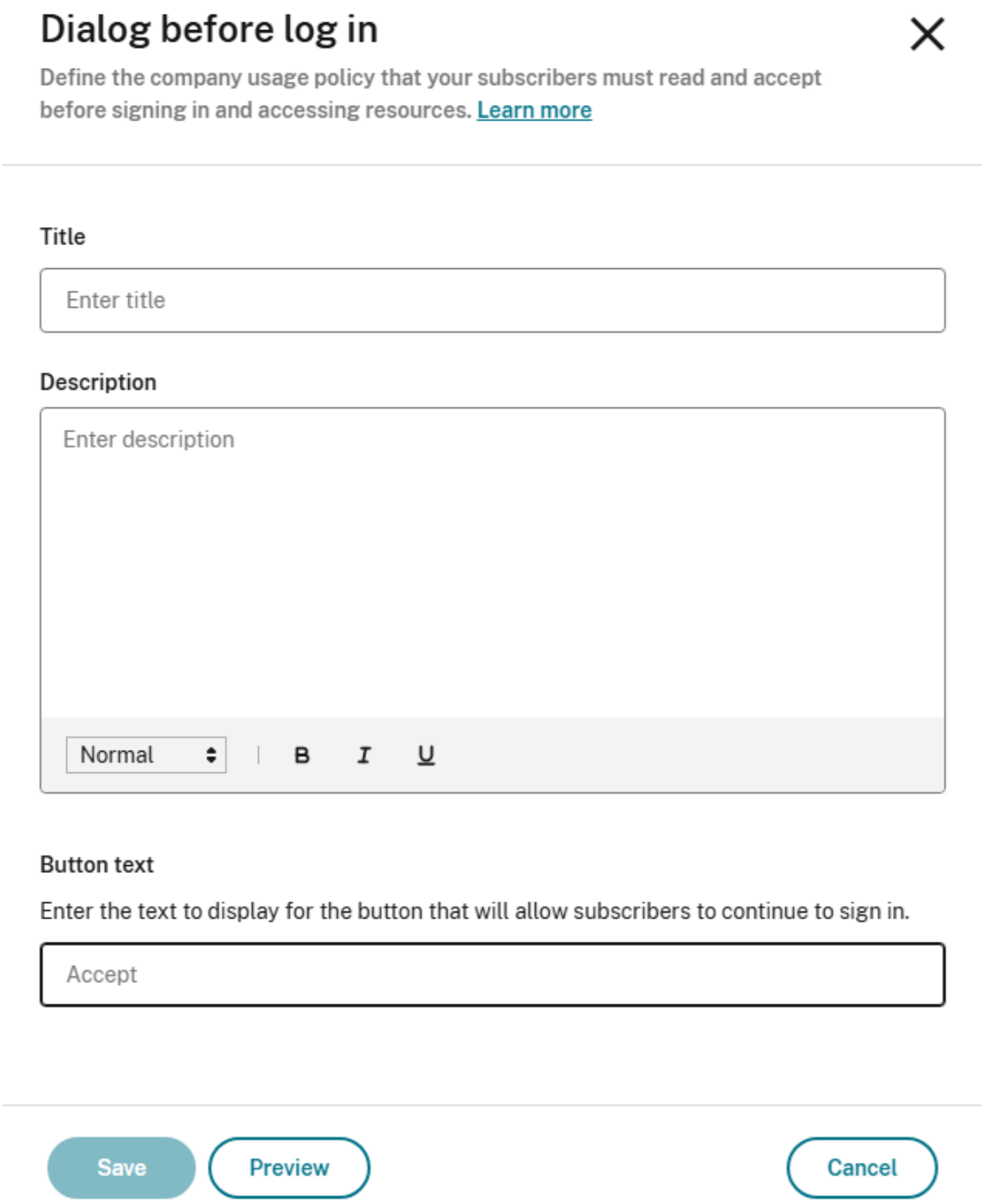
Create a custom dialog that is displayed before users log in. It is displayed on all clients including web, desktop and mobile devices. You can use it to display information such as company usage policy, or an upcoming maintenance window. Users must accept the dialog before proceeding to the log in screen.

1. If not enabled, select the toggle labelled **Before log in**. If it is already enabled, click the **Edit** button.




2. A configuration dialog will appear.
3. Enter the **Title** for the dialog.
4. Enter the **Description** to be displayed in the dialog. It is not possible to localize the text, however you can append multiple different languages within the description.
5. Enter the **Button text**. The users must press this button to proceed.




6. Select **Preview** to see what the dialog looks like for end users.
7. When you're finished, select **Save**.

For the end user experience, see End user experience - Before log in dialog.

> **Note**
>
> If you have Citrix Gateway configured as your store identity provider, you might already have a log in policy as part of your AAA and nFactor authentication flow. Citrix recommends that you configure only one log in policy, either as part of your existing nFactor authentication flow or outside the flow using the Citrix Cloud administration console.

### Configure a custom dialog to be displayed after log in

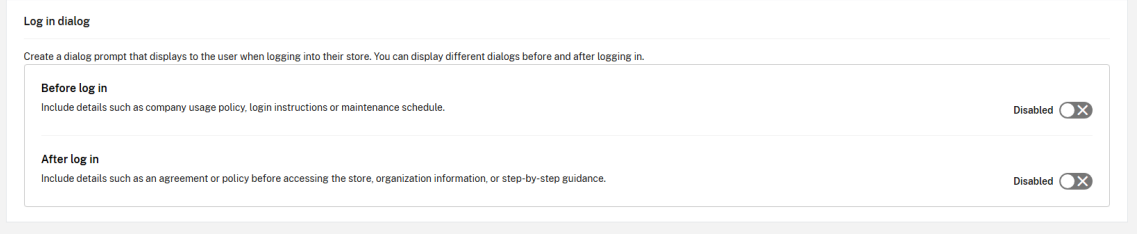
You can configure a custom dialog that is displayed after users log in. It is displayed on all clients including web, desktop, and mobile devices. You can use it to display information such as company usage policy, or an upcoming maintenance window. Users must accept the dialog before proceeding to their resources.

The admin can decide how often the dialog is shown on a per-device basis that is, only once, every day, every 7 days, or every 30 days.

> **Note:**
>
> When the user clears caches and cookies it makes the dialog to appear again.

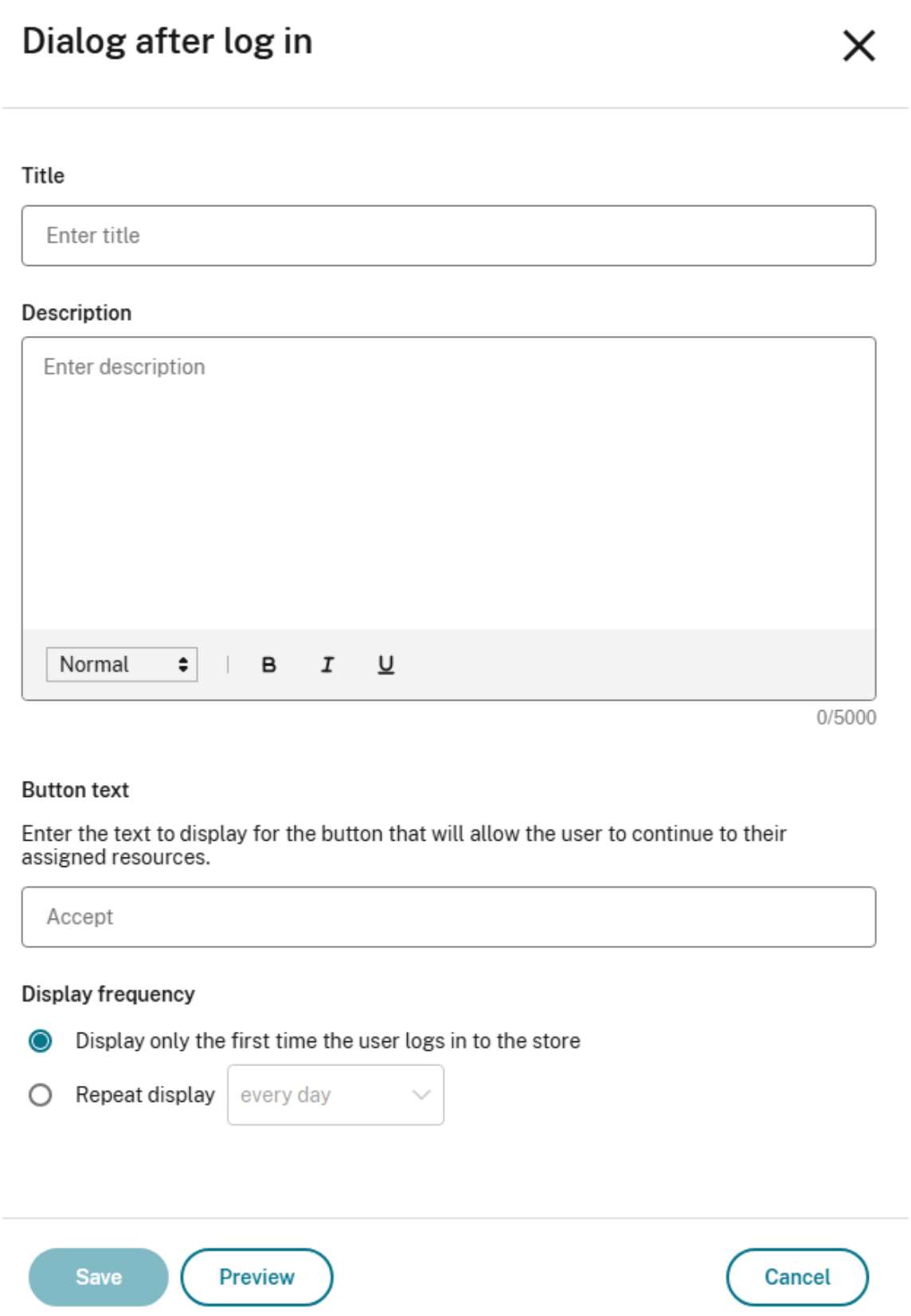
1. If not enabled, select the toggle labeled **After log in** to enable. If it is already enabled, click the **Edit** button.

   A configuration dialog appears.




2. Enter the **Title** for the dialog.
3. Enter the **Description** to be displayed in the dialog. It is not possible to localize the text. However, you can append multiple different languages within the description.
4. Enter the **Button text**. The users must press this button to proceed.
5. Enter a choice for display frequency for how often each user sees the dialog.



6. Select **Preview** to see what the dialog looks like for end users.
7. After the self-review, select **Save**.

For the end user experience, see End user experience - After log in dialog.

## Integrate services into stores

June 22, 2026

This article outlines the steps involved in adding services to Citrix® StoreFront Cloud, which is a two-step process:

1. Configure individual services in Citrix Cloud. You can find a list of Citrix Cloud services that link to instructions for each one in Citrix Cloud Services.
2. Enable (and disable) access to your configured services in **StoreFront Cloud** > **Service Integrations**.

### Configure services

Your purchased services are displayed in a card layout in the Citrix Cloud™ dashboard. Services that you've purchased include a **Manage** button.

To configure purchased services:

1. Sign in to Citrix Cloud.
2. Select **Manage** in the tile of the service that you want to configure.
3. Follow the instructions for setting up that service.

For a brief description of cloud-hosted services, visit Cloud-hosted services through Citrix® StoreFront Cloud.

If you'd like to try a new service, you can request a trial or demo. For more information on service trials, visit Citrix Cloud Service Trials.

### Enable services

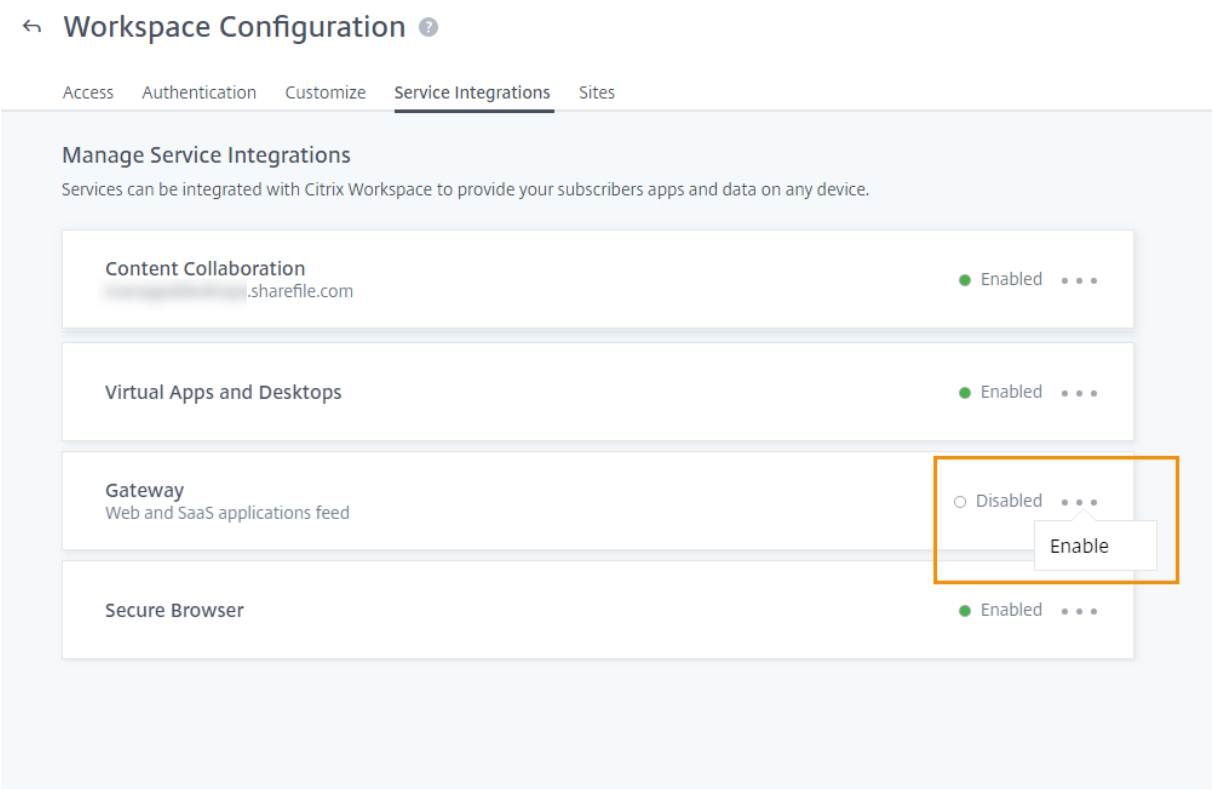
Once you've configured your services, you can integrate them into Citrix® StoreFront Cloud.

Subscribing to **DaaS** and the **Remote Browser Isolation service** enables them by default. All other new services that your organization subscribes to are disabled by default.

To enable Citrix® StoreFront Cloud integration for a service:

1. Navigate to **StoreFront Cloud** > **Service Integrations**.
2. Select the ellipses button next to the service and then select **Enable**.



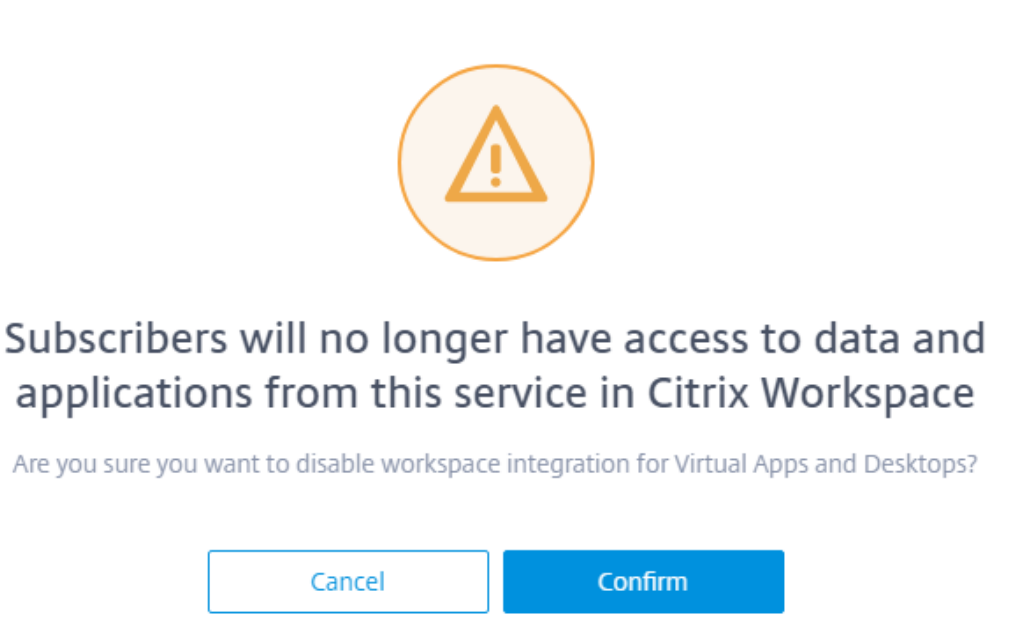

## Disable services

Disabling Citrix® StoreFront Cloud integration blocks end user access for that service. This doesn't disable the store URL, but end users can't access data and applications from that service in Citrix® StoreFront Cloud.

To disable Citrix® StoreFront Cloud integration for a service:

1. Navigate to **StoreFront Cloud** > **Service Integrations**.
2. Select the ellipses button next to the service and then select **Disable**.
3. When prompted, select **Confirm** to acknowledge that end users won't have access to data or applications from the service.




# Optimize DaaS in Citrix® StoreFront Cloud

June 22, 2026

You can improve the efficiency and availability of your DaaS apps and desktops with the following options:

- Make your existing, on-premises virtual apps and desktops deployment available to store end users with site aggregation.
- Optimize connectivity with Direct Workload Connection, which involves configuring network locations in Citrix Cloud.
- Ensure service continuity during an outage for offline resilience.
- Configure single sign-on (SSO) to DaaS with Citrix Federated Authentication Service (FAS).

## Site aggregation

Site aggregation allows you to add your on-premises virtual apps and desktops deployment to your store so that end users can access these resources alongside cloud-managed resources.

For more information on site aggregation, see Aggregate on-premises virtual apps and desktops in stores.

For more information on scalability limits, see store platform scalability limits.

### Direct Workload Connection

Direct Workload Connection uses network locations to switch between internal and external routes to the virtual machines that host your virtual apps and desktops.

With Direct Workload Connection, you allow clients inside your corporate network to switch to direct launches of Citrix DaaS. Direct launches don't require the HDX connections between clients and VDAs to be proxied through a gateway. Direct Workload Connection requires at least one internal network location.

For more information, visit Optimize connectivity with Direct Workload Connection.

### Service continuity

Service continuity ensures that end users maintain access to critical apps and desktops through Citrix Workspace app if there's a Citrix Cloud™ outage.

Service continuity stores connection leases on client disks that have Citrix Workspace app installed. Connection leases are refreshed periodically when clients access the store. Clients can then launch Citrix DaaS that they could access before the outage. For more information, visit Service continuity.

### Citrix Federated Authentication Service (FAS)

Citrix® StoreFront Cloud supports using Citrix Federated Authentication Service (FAS) for single sign-on (SSO) to Citrix DaaS. FAS allows end users using a federated identity provider, such as Microsoft Entra ID or Okta, to enter their credentials only once when they sign in to their stores. Without FAS, end users using a federated identity provider are prompted to enter their credentials more than once to access their virtual apps and desktops.

Using FAS with store has the following requirements:

- A FAS server configured as described in the Requirements section of the FAS product documentation.
- A connection between your FAS server and Citrix Cloud, created through the **Connect to Citrix Cloud** option in the FAS installer.
- A connection between your on-premises Active Directory domain and Citrix Cloud, with FAS enabled in **StoreFront Cloud**.

For information about implementing FAS, see Enable single sign-on for stores with Citrix Federated Authentication Service.

### Resource filtering

Citrix® StoreFront Cloud passes information on the store used to DaaS, which you can use to filter resources. For more information, see Resource filtering using delivery group access policies

## Aggregate on-premise Citrix Virtual Apps and Desktops™ sites

June 22, 2026

You can add your on-premise Citrix Virtual Apps and Desktops site to Citrix® StoreFront Cloud to make your existing apps and desktops available to end users. After adding your site, users can access all their virtual apps and desktops alongside other resources, when they sign in to their store. This process is known as *on-premise site aggregation*. For external connectivity to VDAs, you can use your own Citrix Gateway or use the Citrix Gateway service.

> **Important:**
>
> Citrix® only recommends on-premise site aggregation for small deployments where there is no need for Service continuity. For more information, see limitations. As an alternative, consider migrating the sites to Citrix DaaS™, or deploy StoreFront™.

This article covers only on-premise sites. For information on aggregating multiple DaaS sites, refer to Multi-site management and end-user resource aggregation.

### Limitations

Service continuity and Local Host cache are not available for on-prem sites aggregated by Citrix® StoreFront Cloud.

The following scalability limits apply:

| SLI metric | SLO threshold limit |
|---|---|
| Concurrent end users for all aggregated on-prem Citrix Virtual Apps and Desktops sites | 500 |
| Number of on-prem Citrix virtual apps and desktops sites | 4 |

Above 4 sites, users might experience slow response times.

## Prerequisites

### Citrix Virtual Apps and Desktops

For minimum supported versions of Citrix Virtual Apps and Desktops, see System requirements.

If using an authentication method other than Active Directory username and password, or Active Directory username and password with token, enable XML trust.

### Federated Authentication Service

If you require Federated Authentication Service (FAS) for single sign-on to VDAs then you must connect your FAS servers to Citrix Cloud™. For more information, see Enable single sign-on for stores with Citrix Federated Authentication Service.

### Cloud Connectors

Cloud Connectors allow Citrix Cloud to locate and communicate with your site. For minimal interruption, Citrix recommends installing Cloud Connectors before adding your site to Citrix® StoreFront Cloud.

For high availability, Citrix recommends at least two (2) servers on which to install Citrix Cloud Connector™ software. These servers must:

- Meet the system requirements described in Cloud Connector Technical Details.
- Be joined to your site domain. If users access your site's applications in multiple domains, install at least two Cloud Connectors in each domain.
- Connect to a network that can contact your site.

For more information about installing Cloud Connectors, see Cloud Connector Installation.

### Web proxy configuration

If you have a web proxy in your environment, check that the Cloud Connectors can validate connectivity to the XML Service in your site. Add each XML server within the site to the bypass proxy list on each Cloud Connector. Don't use wildcards or IP addresses because the Cloud Connector supports handling FQDNs only.

1. Add the XML servers to the bypass proxy list:
    a) On the Cloud Connector, select **Start** and then type **Internet Options**.
    b) Select the **Connections** tab and then select **LAN Settings**.

c) Under **Proxy server**, select **Advanced**.
d) Under **Exceptions**, add the FQDN of each XML server in your site using lowercase letters. If these entries use mixed-case or uppercase letters, site aggregation might fail. For more information, see CTX272160 in the Citrix Support Knowledge Center.

2. Import the list so that the Cloud Connector services can consume them. At the command prompt, type `netsh winhttp import proxy source=ie`.
3. From the **Services** console, restart all Citrix Cloud services on each machine hosting the Cloud Connector or restart each machine.

#### Active Directory

If you have separate user and resource forests in Active Directory, you must have Cloud Connectors installed in each forest before you add your on-premises site. Citrix Cloud detects these forests during the site discovery process through the Cloud Connectors. You can then use the forests' users and resources to create stores for your users.

Limitations:

When adding your site, you can't use separate user and resource forests when you define the resource location. Because Cloud Connectors don't participate in any cross-forest trusts that might be established, Citrix Cloud can't discover your site through the Cloud Connectors in these forests. You can use these forests when you define a secondary resource location that provides a different connectivity option for your users. For more information, see Add IP ranges for different connectivity options.

Untrusted forests aren't supported for site aggregation. Although Citrix Cloud and Citrix® StoreFront Cloud support users from untrusted forests, these users can't use cloud stores after an on-premises site is added through site aggregation. Only users located in the forests that the site trusts can sign in and use the store. If users from an untrusted forest try to sign in to the store, they receive the error message, "Your logon has expired. Please log on again to continue."

#### Internal and external connectivity to store resources

During the process of adding your site to Citrix® StoreFront Cloud, you can specify if you want to provide internal or external access to the resources available to users. If you intend to allow only internal users to access your site cloud stores, users must be on the same network as the site to access applications.

If you intend to allow external users to access these resources, you have the following options:

- Use your existing Citrix Gateway to handle the traffic between your on-premises site and Citrix Cloud. Your Citrix Gateway must be configured to use Cloud Connectors as the Secure Ticket

Authority (STA) servers **before** you add your Site to Citrix® StoreFront Cloud. For instructions, see CTX232640.

- Use the Citrix Gateway service to allow Citrix to handle the traffic between your site and Citrix Cloud for you. You can activate a service trial and configure the service when you add your site. If you've already signed up for the Citrix Gateway service, Citrix Cloud detects your subscription when you select this option.

> **Note:**
>
> For Citrix Cloud to detect your Citrix Gateway service subscription, you must use the same OrgID you used when you signed up for the Citrix Gateway service. For more information about OrgIDs in Citrix Cloud, see What is an OrgID?

#### Credentials and ports for site discovery

During the process of adding your site to Citrix® StoreFront Cloud, Citrix Cloud discovers your site and checks that the Controller you specify is available. Before you add your on-premises site, check that you have Citrix administrator credentials with a minimum of **Read Only** permissions. During the site discovery process, Citrix Cloud prompts you to supply these credentials. Citrix Cloud doesn't store these credentials or use them to change to your site.

### Add site

When you add your on-premises site to Citrix® StoreFront Cloud, the **Add Site** wizard guides you through the following steps:

1. Discover your site and select the resource location you want to use.
2. Detect the Active Directory domains in which your Cloud Connectors are installed.
3. Specify the connectivity that you want to use between Citrix Cloud and your site.

#### Step 1: Discover site

In this step, you provide the information that Citrix Cloud needs to locate your site and select your resource location. The resource location specifies the domain and connectivity option for all users who access your site. If you need to install Cloud Connectors in your site's domain, you can do so now. If you already have Cloud Connectors installed, you can select them when prompted.

1. From the Citrix Cloud menu, navigate to **StoreFront Cloud > Sites > Add Site**.
2. Select the type of on-premises site you want to add and continue.

   Citrix Cloud attempts to discover any resource locations and Cloud Connectors in your domain and displays a list for you to select from.

3. Perform one of the following actions:

    - If you have no Cloud Connectors installed in your site's domain, select **Install Connector**. Citrix Cloud prompts you to download the Cloud Connector software and complete the installation wizard.
    - If you have Cloud Connectors installed, Citrix Cloud displays the connectors in the domains in which they were detected. Select the resource location that you want to add to Citrix® StoreFront Cloud. This resource location becomes the default resource location.
    - If you have Cloud Connectors installed, but they aren't displayed, select **Detect**.

4. Select the resource location and Cloud Connector pair that you want to use to discover your site.
5. In **Enter Server Address**, add the IP address or FQDN of a Controller in the site, and select **Discover**
6. If prompted, enter the Citrix Administrator credentials for the site.

    Citrix Cloud tests connectivity to verify that your site is reachable. Discovery might take a few minutes to complete, depending on the type and size of the site.

7. If a success message appears indicating that the site has been successfully discovered, select **Continue**.

#### Step 2: Verify Active Directory Connection

In **Verify Active Directory Connection**, Citrix Cloud displays the domains used with your site and whether there are Cloud Connectors installed in those domains.

If there are no Cloud Connectors in a domain, users in that domain can't use cloud stores to access the applications published there. If you only have one Cloud Connector in your domain, you have two options:

- Install more Cloud Connectors by selecting **Install Connector**.
- Continue without installing more Cloud Connectors by selecting **I understand that high availability requires having two connectors installed in each domain**.

If you have local users assigned to applications in your site, select **Download user list (.csv)**.

After verifying your Active Directory connection, select **Continue**.

#### Step 3: Configure connectivity

In this step, you specify whether you want to allow external or internal-only user access to your site through cloud stores. Internal connectivity requires your users to be on the same network as your

site and VDAs that host your published resources. For external connectivity, you can use your existing on-premises Citrix Gateway or you can use the cloud-hosted Citrix Gateway service.

Select one of the following options in **Select connectivity type > Configure Connectivity**:

- **Add Existing Gateway:** Select this option to use your existing Citrix Gateway to provide external access.
- **Citrix Gateway service:** Select this option to activate a service trial or to use your existing subscription with your site.
- **Internal Only:** Select this option if no other configuration is needed.

If **Add Existing Gateway** is selected, perform the following actions:

1. Select **Edit** and enter the public URL of the Citrix Gateway.
2. Verify that Citrix Gateway is configured to use your Cloud Connectors as the STA servers, described in CTX232640.
3. Select **Test STA** and then, when the test is successful, **Continue**. If the test isn't successful, refer to CTX232517 for troubleshooting.

If **Citrix Gateway service** is selected, but the service isn't enabled for your Citrix Cloud account as a service trial or as a purchase, you can select **Start a 60-day trial**. Citrix Cloud enables the service as a trial for you. If the service was enabled at an earlier time, Citrix Cloud detects the service and displays any remaining trial days.

After completing the preceding tasks, select **Continue**.

#### Step 4: Confirm site aggregation

In this step, you confirm site aggregation, which involves reviewing the XML port, XML servers, Active Directory domains, and the connectivity type you chose earlier.

Citrix Cloud displays up to five XML servers it can connect to. If you have more than one XML server in your site but only one is shown, Citrix Cloud displays an alert. To troubleshoot this issue, refer to CTX232516.

1. In **Confirm Site Aggregation**, review the XML port, XML servers, Active Directory domains, and the connectivity type you chose earlier.
2. Select **Save and Finish**. The **Sites** page displays your newly added site.

If you want to specify different XML servers, you can then edit your site to change these values after you select **Save and Finish**.

#### Step 5: Manage service integrations

After adding your first site, you must enable the **Service Integration** for Virtual Apps and Desktops on-premises sites, which is disabled by default. Users can't see resources from the site until you enable it.

1. Navigate to **StoreFront Cloud > Service Integrations > Virtual Apps and Desktops On-Premises Sites** and select the ellipsis to open the site actions menu.
2. Enable the service integration so that end users can sign in to their stores and see resources from the site.

## Change your site configuration

### Rediscover your site

If you add Delivery Controllers to your site or change XML ports, you can verify that your site is still reachable by Citrix® StoreFront Cloud with a rediscovery process.

1. Navigate to **StoreFront Cloud > Sites**, select the ellipsis for the site you want to update, and then select **Edit Site**.
2. In **Server Address**, type the IP address or FQDN of a Delivery Controller in your site and select **Rediscover**.

### Add or modify XML servers

When you add a site to Citrix® StoreFront Cloud, Citrix Cloud automatically detects XML servers in your site and displays up to five XML servers in your configuration. You can add and remove XML servers as needed from your site configuration up to the display limit of five XML servers.

#### To add an XML server

1. Navigate to **StoreFront Cloud > Sites**, select the ellipsis for the site you want to update and select **Edit Site**.
2. In the **XML Servers** section, enter the XML server port and select **Use SSL** if needed.
3. Select a connectivity method:

    - **Load balanced:** This option allows Citrix Cloud to pick a random XML server from the list.
    - **Failover:** This option allows Citrix Cloud to use the listed XML servers in the order that they appear in the list. Only the first XML service in the list is used for launch unless it becomes unavailable, then the second server is used. You can reorder the list by dragging and dropping each server.

4. Select **Save Changes**.

If you experience an error when adding an XML server, refer to CTX232516 for troubleshooting steps.

### Add IP ranges for different connectivity options

If you have VDAs or session hosts in different subnets, you can specify IP ranges with a different connectivity type for each one. Each IP range can also have a different resource location associated with it. For example, you might have one IP range for machines in the EU where users connect internally, one IP range for machines in the EU where users connect through your Citrix Gateway, and one IP range for machines in the US where users connect through the Citrix Gateway service.

1. Navigate to **StoreFront Cloud > Sites**, select the ellipsis button for the site you want to update, and select **Edit Site**.
2. In the **Connectivity** section, select **Add an IP range with a different connectivity option** and enter an IP range in CIDR format.

To create a resource location for your IP range:

1. Select **Add a new Resource Location** and enter a user-friendly name.
2. In **Select your connectivity**, select whether you want to provide internal-only access or allow external access using your Citrix Gateway or the Citrix Gateway service.

To assign an existing resource location to the IP range:

1. Choose **Select an existing resource location**
2. Select the resource location you want to use.
3. If you choose a resource location with only one Cloud Connector installed, select **I understand that high availability requires having two connectors are installed in a resource location.**
4. Select **Add**.

### Add more Active Directory domains

If you install Cloud Connectors in more domains with Active Directory users in your site, you can check they're added to your site configuration in Citrix® StoreFront Cloud.

1. Navigate to **StoreFront Cloud > Sites**, select the ellipsis for the site you want to update, and then select **Edit Site**.
2. Under Active Directory, select **Refresh**.

### Disable Sites

If you no longer want to make your on-premises site available to users in Citrix® StoreFront Cloud, you can disable it. You can disable an individual on-premises site or all on-premises sites you've added to Citrix® StoreFront Cloud.

When sites are disabled, users can't access the on-premises applications in those sites through Citrix® StoreFront Cloud. However, the configuration for those sites is preserved. If you re-enable a site later on, the site's default resource location, domain, XML server, and connectivity settings are kept.

#### Disable an on-premises site

1. Navigate to **StoreFront Cloud > Sites**, select the ellipsis for the site you want to disable and then select **Disable**.
2. A confirmation message appears. Select **Disable** again.

#### Disable all on-premises sites

To disable all sites on the **Sites** page, disable the Citrix Virtual Apps and Desktops service integration. For instructions, see Disable services.

To re-enable an individual on-premises site or to add another site later on, you must first re-enable the store service integration for all sites on the **Service Integrations** page.

### Delete a site from Citrix® StoreFront Cloud

If you no longer want your on-premises site configuration in Citrix® StoreFront Cloud, you can delete the site. When you delete a site, only the configuration for the site in Citrix® StoreFront Cloud is removed. Citrix Cloud doesn't change your site.

To delete a site, navigate to **StoreFront Cloud > Sites**, select the ellipsis for the site you want to remove, and then select **Delete**.

## Service continuity

June 22, 2026

Service continuity allows users to connect to their DaaS apps and desktops when they are unable to connect to Citrix® StoreFront Cloud or DaaS, for example, due to an outage or a network connectivity problem.

Service continuity works by securely caching connection leases (long-lived authorization tokens) on the local device. The first time a user signs in to their store, it saves connection lease files to the user profile for each resource published to the user. Connection lease files are signed and encrypted and are associated with the user and the user's device. By default, the connection lease allows users to access apps and desktops for seven days but you can change this to up to 30 days.

When users exit Citrix Workspace app, Citrix Workspace app closes but the connection leases are retained. You can configure service continuity to delete or retain connection leases when users explicitly logs out of their store by clicking the **Log out** button. By default, connection leases are deleted from user devices when users log out by clicking the **Log out** button.

Service continuity is supported for double hop scenarios when Citrix Workspace app is installed on a virtual desktop.

For an in-depth technical article about Citrix Cloud resiliency features, including service continuity, see Citrix Cloud Resiliency.

> **Note:**
>
> The deprecated Citrix DaaS™ feature called "connection leasing"resembles connection leases in that it improved connection resiliency during outages. Otherwise, that deprecated feature is unrelated to service continuity.

### User device setup

To access resources using Service Continuity during an outage, a user must have previously signed in to the store using Citrix Workspace app or their web browser with Citrix web extension.

To use Citrix Workspace app, users must perform the following steps on their devices:

1. Download and install a supported version of Citrix Workspace app.
2. Add the store URL for your organization to Citrix Workspace app (for example, `https://example.cloud.com`).
3. Log in to the store.

When using a web browser:

1. Download and install a supported version of Citrix Workspace app.
2. Add Citrix web extensions to their browser.
3. Open the store URL in their browser.
4. Log in.

This video shows how to install and use service continuity in browser.

This is an embedded video. Click the link to watch the video

When a user signs into a store for the first time, service continuity downloads connection leases to the user device. Downloading connection leases might take up to 15 minutes for first-time sign-in. Users can continue launching published resources during the download period.

### User experience during an outage

When service continuity is enabled, the user experience during an outage varies depending on:

- The type of outage
- Whether the Citrix Workspace app is configured with domain pass-through authentication
- Whether session sharing is enabled for the app or desktop the user connects to

For some outages, users continue accessing their DaaS with no change to their user experience. For other outages, user might see a change in how Workspace appears or be prompted to take some action.

This table summarizes how service continuity helps users access apps and desktops during different types of outages.

| Where the outage occurs | How service continuity maintains user access | User experience during outage |
|---|---|---|
| Citrix® StoreFront Cloud | Citrix Workspace app enumerates apps and desktops based on local cache on the user device. | Icons for unavailable apps and desktops appear dimmed. Users can still access apps and desktops that have undimmed icons. After clicking an undimmed icon, users might be prompted to reenter their credentials at the VDA. To regain access to all their apps and desktops, users can try to establish their connection to store by clicking the "Reconnect to store" link. |
| Identity provider | Citrix Workspace app enumerates apps and desktops based on local cache on the user device. | Users might be unable to log in to store. Users click the "Use store offline" link to access some apps and desktops in an experience identical to a store service outage. |

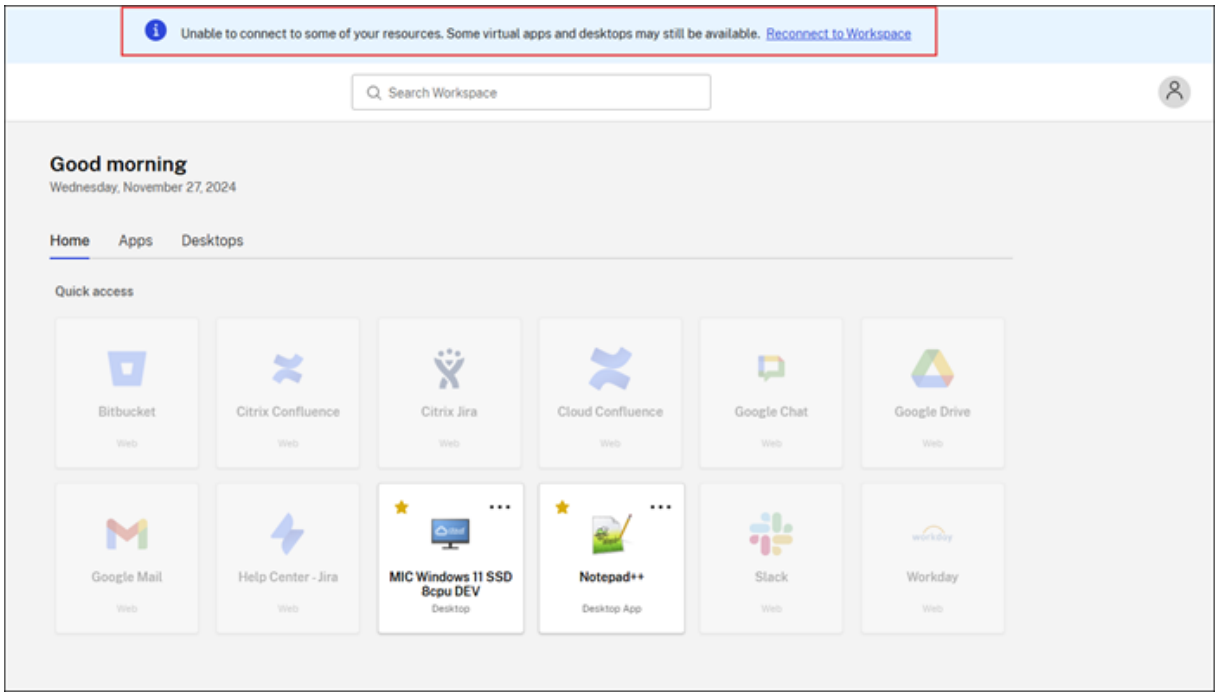
 

| Where the outage occurs | How service continuity maintains user access | User experience during outage |
|---|---|---|
| Citrix Cloud™ Broker Service | For VDAs registered with connectors, the High Availability Service in the Cloud Connector takes over brokering. All VDAs that were registered with the Cloud Broker Service register with the High Availability Service. For connectorless VDAs, the brokering of the session is done through the Virtual Delivery Agent (VDA). | Some users might be unable to access virtual resources while VDAs register with the High Availability Service. Existing sessions aren't affected. No user action needed. |
| Secure Ticket Authority | Connection leases provide access to virtual resources when ICA® files can't. | Sessions launches might take a few seconds longer. No user action needed. |
| Citrix Gateway service | Network traffic fails over to the closest healthy Citrix Gateway service point of presence (POP). | Existing sessions might take a few seconds to reconnect. No user action needed. |
| Internet connection on the LAN | Citrix Workspace app enumerates apps and desktops based on local cache on the user device. If a user has a direct network connection to the resource location, Citrix Workspace app bypasses the Citrix Gateway service when the user clicks undimmed icons. Citrix Workspace app contacts the Cloud Connector over TCP 2598 and contacts VDAs over TCP 2598 or UDP 2598. | Icons for unavailable apps and desktops appear dimmed. Users can still access apps and desktops that have undimmed icons. After clicking an undimmed icon, users might be prompted to reenter their credentials at the VDA. To regain access to all their apps and desktops, users can try to establish their connection to store by clicking the "Reconnect to store" link. |

### Citrix® StoreFront Cloud outage

During a Citrix® StoreFront Cloud outage, users see this message at the top of the Citrix® StoreFront Cloud home page: "Unable to connect to some of your resources. Some virtual apps and desktop may still be available."Users see apps and desktops that they can connect to during the outage. If the app or desktop isn't available, the icon appears dimmed.




To access available resources during an outage, users select a resource icon that isn't dimmed.

### Launching resources

Depending on how Citrix Workspace app and VDAs are configured, during an outage the VDA might prompt users to enter their credentials into the Windows Logon user interface. If this prompt occurs, users enter their Active Directory (AD) credentials or smart card PIN to access the app or desktop.

Users can access resources without entering their AD credentials if Citrix Workspace app for Windows is configured with domain pass-through authentication. For more information, see Configure single sign-on using the graphical user interface.

If session sharing is enabled, users can access apps or desktops hosted on the same VDA after they provide their credentials for one resource on that VDA. Session sharing is configured for the application group containing the resource on the VDA. For information about configuring application groups, see Create application groups.

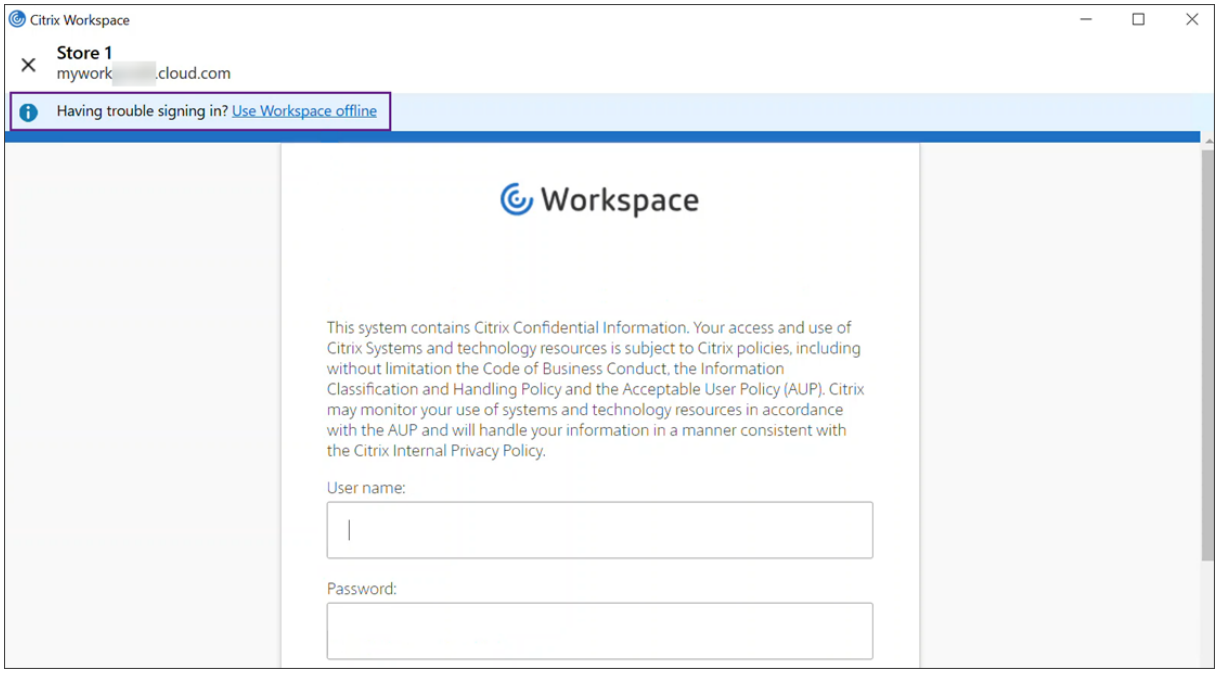
In all other configurations, users are prompted to reenter their AD credentials at the VDA before accessing resources.

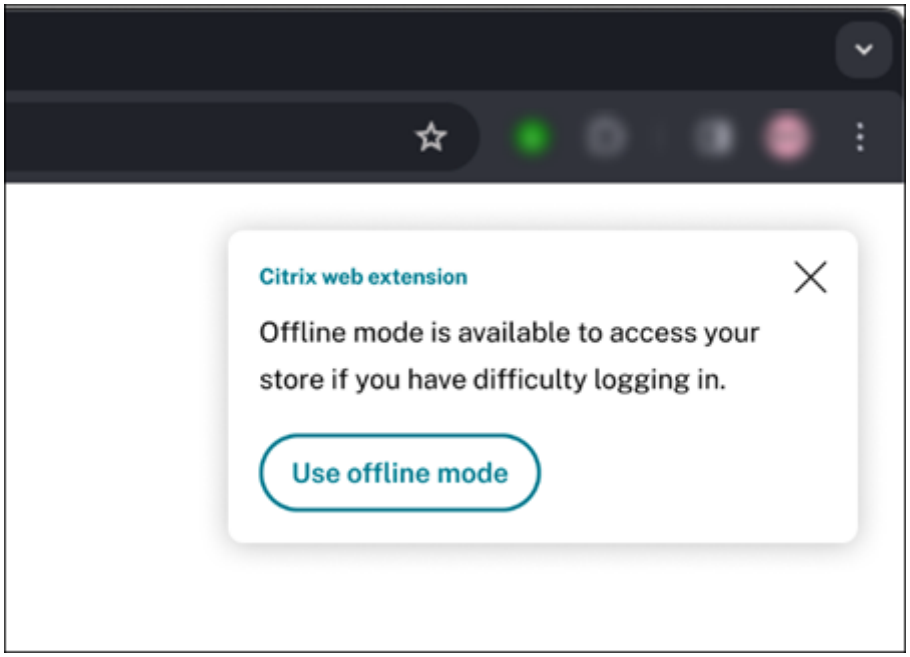
### Identity provider outages

During an outage in the identity provider for store authentication, users might be unable to log in to their store through the store log in page.

When using Citrix Workspace app, after 40 seconds, this message appears at the top of the window.




If using a web browser, after 60 seconds the following pop-up appears.




Afterward, the store home page appears. Users then access resources as they would during a Citrix®

StoreFront Cloud outage.

#### Exit and log out behavior

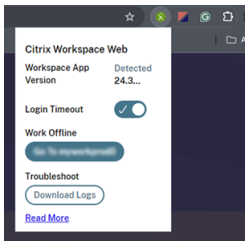
Regardless of the type of outage, users can continue to access resources if they exit and relaunch Citrix Workspace app or browser including after restarting their devices.

In the default configuration of service continuity, users lose access to their resources if they explicitly log out of the store. If you want users to retain access to their resources after signing out, specify that connection leases are kept when users log out. See Configure service continuity.

#### Browser user experience during outages

To access available apps and desktops offline, users can click **Use offline mode**.

To manage the offline mode prompt, click the Citrix web extension in the browser on the user device. The following screen appears:




Users can use the **Work Offline** option to manually switch to offline mode without waiting 60 seconds for the offline mode prompt.

During some outages, the warning window prompting users to work offline appears automatically when the extension detects store-side issues. The user doesn't need to take any action or wait through the login timeout interval.

### Requirements and limitations

#### Site requirements

- Supported in all editions of Citrix DaaS with Citrix® StoreFront Cloud.
- Not supported for Citrix® StoreFront Cloud with site aggregation to on-premises Virtual Apps and Desktops.
- Not supported when on-premises Citrix Gateway is used as an ICA Proxy. (Using Citrix Gateway Service as a store authentication method is supported.)

### User device requirements

Minimum supported Citrix Workspace app versions:

- Citrix Workspace app for Windows 2106
- Citrix Workspace app for Linux 2106
- Citrix Workspace app for Mac 2106
- Citrix Workspace app for Android 22.2.0
- Citrix Workspace app for iOS 22.4.5
- Citrix Workspace app for ChromeOS 2301

For users who access their apps and desktops using browsers:

- Citrix Workspace app 2109 for Windows at a minimum. Supported with Google Chrome and Microsoft Edge.
- Citrix Workspace app for Mac version 2112 at a minimum for use with Google Chrome.
- Citrix Workspace app for Windows (Store) is not supported.

If using connectorless VDAs:

- Citrix Workspace app for Windows 2309 or later

Only one user per device is supported. Kiosk or "hot desk"user devices aren't supported.

### Web browser requirements and limitations

When accessing a store through a web browser, users must use a browser supported by Citrix web extensions.

If users clear cookies and other site data in their browsers during an outage, service continuity doesn't work until they authenticate to store again.

Service continuity isn't supported in incognito or InPrivate mode.

### Supported store authentication methods

- Active Directory
- Active Directory plus token
- Microsoft Entra ID
- Okta
- Citrix Gateway (primary user claim must be from AD)
- SAML 2.0
- Conditional Authentication

#### Authentication limitations

- Single sign-on with Citrix Federated Authentication Service (FAS) isn't supported. Users enter their AD credentials into the Windows Logon user interface on the VDA.
- Single sign-on to VDA using cached Active Directory credentials isn't supported.
- Local mapped accounts aren't supported.
- VDAs can be Microsoft Entra ID joined, Microsoft Entra hybrid joined, or AD joined.
- If using Adaptive Authentication, the Adaptive Authentication or service must remain reachable for service continuity to function.
- If using the Device Posture service, the Device Posture service must remain reachable for service continuity to function. To maintain security, service continuity verifies the results of the latest scan of the device's posture before launching a session. If the results of the scan are unavailable or outdated, service continuity prevents session launch, ensuring compliance with security policies.
- For connectorless VDAs, signing in with Windows Hello in the virtual desktop is not supported. Only user name and password are currently supported. If users try to log in with any Windows Hello method, they receive an error stating that they are not the brokered user, and the session is disconnected. Associated methods include PIN, FIDO2 key, MFA, and so on.

#### Citrix Cloud Connector™ scale and size

- 4 vCPU or more
- 6 GB memory or more

#### Citrix Cloud Connector connectivity

Citrix Cloud Connector must be able to reach `https://rootoftrust-ap-s.apps.cloud.com`, `https://rootoftrust-eu.apps.cloud.com`, and `https://rootoftrust.apps.cloud.com`. For more information, see System and Connectivity Requirements in Citrix Cloud documentation. Configure your firewall to allow this connection. For information about the Cloud Connector firewall, see Cloud Connector Proxy and Firewall Configuration.

#### Connectivity optimization limitations

Advanced Endpoint Analysis (EPA) isn't supported.

Enlightened Data Transport (EDT) isn't supported during outages.

### VDA requirements and limitations

- VDAs registered with connectors: 7.15 LTSR or higher. For connectorless VDAs: 2402 or higher.
- VDAs must be online for users to access VDA resources during an outage. Service continuity does no protect against outages of platforms hosting the VDAs such as Azure or AWS.
- For VDAs registered with connectors, workloads supported during outages:
  - Hosted shared apps and desktops
  - Random non-persistent desktops (pooled VDI desktop) with power management
  - Static non-persistent desktops
  - Static persistent desktops, including Remote PC Access

  > **Note:**
  >
  > Assign on first use isn't support during outages. Random non-persistent desktops with power management are unavailable by default if Cloud Connectors lose connectivity with Citrix Cloud unless `ReuseMachinesWithoutShutdownInOutage` is configured for the delivery group. Review Application and desktop support for more details.

- For connectorless VDAs using Rendezvous V2, workloads supported during outages:
  - Static persistent desktops

For more information about available VDA functions during outages, see VDA management during outages.

### Local keyboard mapping requirements and limitations

The Windows Logon user interface that prompts users to reauthenticate on the VDA does not support local keyboard language mapping. To allow users to reauthenticate during an outage if they have local keyboard language mapping on their devices, preload the keyboard layouts these users require.

> **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.

Edit this registry key in the VDA image:

`HKEY_USERS\.DEFAULT\Keyboard Layout\Preload`

The corresponding language pack in the virtual desktop image must be installed.

For a list of keyboard identifiers associated with keyboard languages, see Keyboard Identifiers and Input Method Editors for Windows.

## Configure resource location network connectivity for service continuity

You can configure your resource location to accept connections from inside your LAN, outside your LAN, or both.

### Configure for connections inside your LAN

1. From the Citrix Cloud menu, go to **StoreFront Cloud > Access**.
2. Select **Configure Connectivity**.
3. Select **Internal Only** as your connectivity type.
4. Click **Save**.

Configure your Citrix Cloud Connector and VDA firewalls to accept connections over Common Gateway Protocol (CGP) TCP port 2598. This configuration is the default setting.

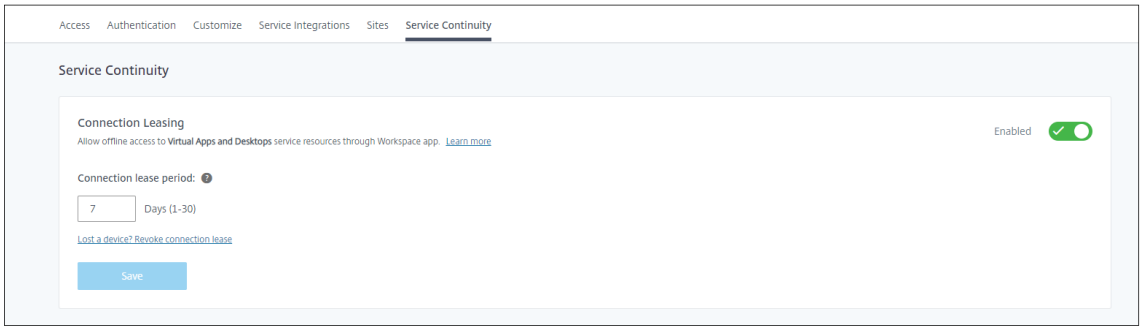
### Configure for connections from outside your LAN

1. From the Citrix Cloud menu, go to **StoreFront Cloud > Access**.
2. Select **Configure Connectivity**.
3. Select **Gateway Service** as your connectivity type.
4. Click **Save**.

## Configure service continuity

To enable service continuity for your site:

1. From the Citrix Cloud menu, go to **StoreFront Cloud > Service Continuity**.
2. Set **Connection leasing for the store** to **Enable**.



3. Set **Connection lease period** to the number of days a connection lease can be used to maintain a connection. The connection lease period applies to all connection leases through your site. The connection lease period starts the first time a user signs in to the store. Connection leases are refreshed each time the user signs in, up to once a day. The connection lease period can be from one day to 30 days. The default is seven days.
4. Click **Save**.

When you enable service continuity, it is enabled for all delivery groups in your site. To disable service continuity for a delivery group, use the following PowerShell command:

```
Set-BrokerDesktopGroup -name <deliverygroup> -ResourceLeasingEnabled $false
```

Replace `deliverygroup` with the name of the delivery group.

By default, connection leases are deleted from the user device if the user logs out of their store during an outage. If you want connection leases to remain on user devices after users log out, use the following PowerShell command:

```
Set-BrokerSite -DeleteResourceLeasesOnLogOff $false
```

> **Notes:**
>
> - Connection leases can't be set to remain on user devices after users log out for users connecting with Citrix Workspace app for Mac. Citrix Workspace app for Mac is unable to read the value of the `DeleteResourceLeaseOnLogOff` property.
> - It might take up to 12 hours for Workspace app clients to update after the setting is configured.

#### Configure Service Continuity for connectorless workloads

Service Continuity for connectorless workloads must be configured per resource location.

1. Install VDA 2402 for Microsoft Entra ID joined VDAs.

   a) Enable the CLXMTP service on the VDAs by configuring the following registry key, then reboot the VDA:

```
[HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\ClxMtpService]
"ClxMtpSvcEnabled"=dword:00000001
"ClxMtpTimeoutInMilliSeconds"=dword:00035000
"ClxMtpFsmLogLevel"=dword:00000003
```

   > **Note:**

> For MCS provisioned VDAs, consider setting these registry keys on the master image

2. Create a Microsoft Entra ID joined catalog.
3. Create a Delivery Group.

> **Note**
>
> Only dedicated desktops are supported. Assign the desktop to a user.

4. Enable Service Continuity.
5. Enable Service Continuity for connectorless workloads on the connectorless resource location by running the following PowerShell.

```
powershell
Set-ConfigZone -Name <zoneName> -
   EnableVdaConnectivityForResourceLeases $true
```

### How service continuity works

If there's no outage, users access virtual apps and desktops using ICA files. Citrix® StoreFront Cloud generates a unique ICA file each time a user selects a virtual app or desktop icon. Each ICA file contains a Secure Ticket Authority (STA) ticket and a logon ticket that can be redeemed only once to gain authorized access to virtual resources. The tickets in each ICA file expire after about 90 seconds. After the ticket in an ICA file is used or expires, the user needs another ICA file from Citrix® StoreFront Cloud to access resources. When service continuity isn't enabled, outages can prevent users from accessing resources if Citrix® StoreFront Cloud can't generate an ICA file.

Citrix® StoreFront Cloud generates ICA files when users launch virtual apps and desktops regardless of whether service continuity is enabled. When service continuity is enabled, Citrix® StoreFront Cloud also generates the unique set of files that make up a connection lease. Unlike ICA files, connection lease files are generated when the user signs into their store, not when the user launches the resource. When a user signs in to their store, connection lease files are generated for every resource published to that user. Connection leases contain information that gives the user access to virtual resources. If an outage prevents a user from signing in to their store or accessing resources using an ICA file, the connection lease provides authorized access to the resource.

### How sessions launch during outages

When users click an icon for an app or desktop during an outage, Citrix Workspace app finds the corresponding connection lease on the user device. Citrix Workspace app then opens a connection. If connectivity to the resource location that hosts the app or desktop is configured to accept connections

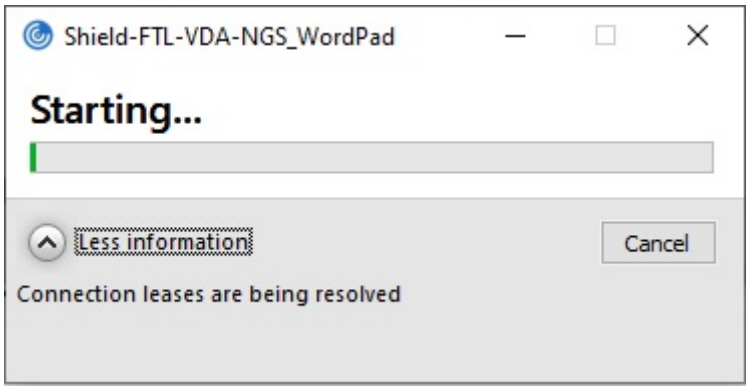
from outside your LAN, a connection opens to Citrix Gateway Service. If you configure connectivity to the resource location that hosts the app or desktop to accept connections from inside your LAN only, a connection opens to the Cloud Connector.

When opening the store in a web browser, the browser uses Citrix web extension to communicate with Citrix Workspace app using the native messaging host protocol for browser extensions.

When the Citrix Cloud broker is online, the Cloud Connector uses the Citrix Cloud broker to resolve which VDA is available. When the Citrix Cloud broker is offline, the secondary broker for the Cloud Connector (also known as the High Availability service) listens for and processes connection requests.

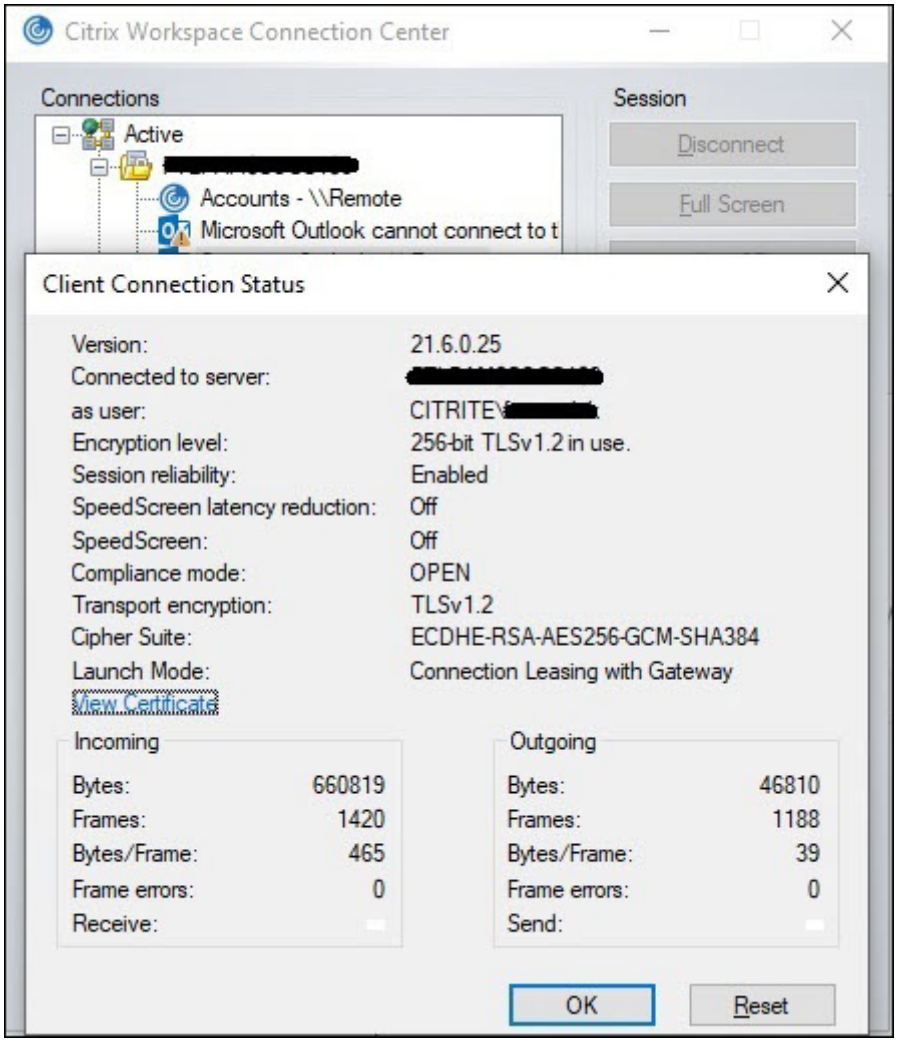
Users who are connected when an outage occurs can continue working uninterrupted. Reconnections and new connections experience minimal connection delays. This functionality is similar to Local Host Cache, but does not require an on-premises StoreFront.

When a user launches a session during an outage, this window appears indicating that connection leases were used for the session launch:




After the user has finished signing into the session, these properties appear in the store Connection Center:




The launch mode property provides information about the connection leases used to launch the session.

On devices running Citrix Workspace app for Mac, Citrix Viewer displays information showing that connection leases were used for the session launch:


### What makes it secure

All sensitive information in the connection lease files is encrypted with the AES-256 cipher. Connection leases are bound to a public/private key pair uniquely associated with the specific client device and can't be used on a different device. A built-in cryptographic mechanism enforces use of the unique key pair on each device.

Connection leases are stored on the user device in AppData\Local\Citrix\SelfService\ConnectionLeases.

The security architecture of service continuity is built on public-key cryptography, similarly to a public key infrastructure (PKI), but without certificate chains and certificate authorities. Instead, all the components establish transitive trust by relying on a new Citrix Cloud service called the root of trust that acts like a certificate authority.

#### Block connection leases

If a user device is lost or stolen, or a user account is closed or compromised, you can block connection leases. When you block connection leases associated with a user, the user can't connect to resources. Citrix Cloud no longer generates or synchronizes connection leases for the user.

When you block connection leases associated with a user account, you block connections to that account on all devices associated with it. You can block connection leases for a user or for all users in a user group.

To revoke connection leases for a single user or user group, use this PowerShell command:

```
Set-BrokerConnectionLeaseRevocationDate -Name username -LeaseRevocationDays
 Days
```

Replace `username` with the user associated with the account you want to block from connecting. Replace `username` with a user group to block connection from all accounts in the user group. Replace `Days` with the number of days connections are blocked.

For example, to block connections for xd.local/user1 for the next 7 days, type:

```
Set-BrokerConnectionLeaseRevocationDate -Name xd.local/user1 -
    LeaseRevocationDays 7
```

To view the time period for which connection leases are revoked, use this PowerShell command:

```
Get-BrokerConnectionLeaseRevocationDate -Name username
```

Replace `username` with the user or user group you want to view the time period for.

For example, to view the time period for which connection leases are revoked for xd.local/user1, type:

```
Get-BrokerConnectionLeaseRevocationDate -Name xd.local/user2
```

This information appears:

```
FullName                          :
Name                              : XD\user2
UPN                               :
Sid                               : S-1-5-21-nnnnnn
LeaseRevocationDays               : 2
LeaseRevocationDateTimeInUtc      : 2020-12-17T17:34:25Z
LastUpdateDateTimeInUtc           : 2020-12-19T17:34:25Z
```

From this output, you can see that user xd.local/user2 has connection leases revoked for two days, from December 17, 2020, through December 19, 2020, at 17:34:25 UTC on each day.

To allow a user account that has connection leases revoked to receive connection again, remove the block using this PowerShell command:

```
Remove-BrokerConnectionLeaseRevocationDate -Name username
```

Replace `username` with the blocked user or user group you want to receive connection. To allow all blocked user account to receive connections, leave out the `Name` option.

### Double hop scenarios

Service continuity can allow users to access virtual resources during outages in double hop scenarios if they're signed in to their store before the outage occurs. In a double hop scenario, a physical user device connects to a virtual desktop that has Citrix Workspace app installed. The virtual desktop then connects to another virtual resource.

In the double hop scenario, service continuity can allow users to access virtual resources during an outage regardless of the type of virtual desktop. If the virtual desktop retains user changes, service

continuity can also provide access to virtual resources during outages that occur while the user isn't signed in.

Service continuity treats the physical user device and the virtual device in a double hop scenario as individual client endpoints. Each device has its own set of connection leases. When a user signs in to a store on a physical device, connection lease files are downloaded and saved to the user profile on the physical device. The user then accesses a virtual desktop and signs in to a store on the virtual desktop. At this point, a different set of connection leases is downloaded and saved the user profile on the virtual desktop. Connection lease files are associated with the device they're downloaded to. Connection lease files can't be copied to another device and reused, even by the same user. Thus, service continuity can't provide access to resources during outages that occur after the session ends if the virtual desktop discards changes made during a user session. For this type of virtual desktop, connection leases are among the changes discarded.

Here's how service continuity works in double hop scenarios with each type of supported virtual desktop.

| For double hops that include… | Service continuity can provide access to virtual resources during outages… |
|---|---|
| Hosted shared desktops | If the outage occurs while the user is signed in to the virtual desktop. |
| Random non-persistent desktops (pooled VDI desktop) | If the outage occurs while the user is signed in to the virtual desktop. |
| Static non-persistent desktops | If the virtual desktop hasn't restarted since the user last logged in. |
| Static persistent desktops | Anytime an outage occurs. |

### VDA management during outages

For VDAs registered with connectors, service continuity uses the Local Host Cache function within the Citrix Cloud Connector. Local Host Cache allows connection brokering to continue on a site when the connection between the Cloud Delivery Controller and the Cloud Connector fails. Because service continuity relies on Local Host Cache, it shares some limitations with Local Host Cache.

> **Note:**
>
> Although service continuity uses Local Host Cache within the Cloud Connector, unlike Local Host Cache, service continuity isn't supported with on-premises StoreFront.

Service Continuity for connectorless workloads differs from Service Continuity in that the brokering of the session is done through the Virtual Delivery Agent (VDA) rather than Cloud Connectors. The VDA

communicates with the Citrix Cloud back end services to broker the session for the user through either a direct connection or the Gateway Service, depending on the settings configured for that resource location. More information regarding how resource location network connectivity can be configured for Service Continuity can be found in Configure resource location network connectivity for service continuity.

#### Power management of VDAs during outages

If Cloud Connectors lose connectivity to Citrix Cloud, Connectors are unable to receive hypervisor credentials from Citrix Cloud. This means:

- During an outage, all machines are in the unknown power state and no power operations can be issued. However, VMs on the host that are powered-on can be used for connection requests.

By default, power-managed desktop VDAs in pooled delivery groups that have the **ShutdownDesktopsAfterUse** property enabled are not available for new connections if Cloud Connectors lose connectivity with Citrix Cloud. You can change this setting to allow those desktops to be used if Cloud Connectors lose connectivity with Citrix Cloud by configuring the `ReuseMachinesWithoutShutdownInOutage` flag on your delivery groups. Changing the `ReuseMachinesWithoutShutdownInOutage` parameter to $true can result in data from previous user sessions to be present on the VDA until it is restarted.

Power management resumes when normal operations resume after an outage.

#### Machine assignment and automatic enrollment

An assigned machine can be used only if the assignment occurred during normal operations. New assignments cannot be made during an outage.

Automatic enrollment and configuration of Remote PC Access machines isn't possible. However, machines that were enrolled and configured during normal operation are usable.

#### VDA resources in different zones

Server-hosted applications and desktop users might use more sessions than their configured session limits, if the resources are in different zones.

Unlike Local Host Cache, service continuity can launch apps and desktops from registered VDAs in different zones, providing the resource is published in more than one zone. Citrix Workspace app might take longer to find a healthy zone as it cycles sequentially through all the zones in the connection lease.

## Monitoring and troubleshooting

Service continuity performs two main actions:

- Download connection leases to the user device.  connection leases are generated and synced with the Citrix Workspace app.
- Launch virtual desktops and apps using connection leases.

### Troubleshooting downloading connection leases

You can view connection leases at this location on the user device.

On Windows devices:

`C:\Users\Username\AppData\Local\Citrix\SelfService\ConnectionLeases\Store GUID\User GUID\leases`

`Username` is the user name.

`Store GUID` is the global unique identifier of the store.

`User GUID` is the global unique identifier of the user.

On Mac devices:

`$HOME/Library/Application Support/Citrix Receiver/CLSyncRoot`

For example, open `/Users/luca/Library/Application Support/Citrix Receiver/CLSyncRoot`

On Linux:

`$HOME/.ICAClient/cache/ConnectionLease`

For example, open `/home/user1/.ICAClient/cache/ConnectionLease`

Connection leases are generated when the Citrix Workspace app connects to the store. View registry key values on the user device to determine whether the Citrix Workspace app has successfully contacted the connection lease service in Citrix Cloud.

Open regedit on the user device and view this key:

`HKCU\Software\Citrix\Dazzle\Sites\store-xxxx`

If these values appear in the registry key, the Citrix Workspace app contacted or attempted to contact the connection lease service:

- `leaseLastCallHomeTime`
- `leaseLastSyncStatus`

If the Citrix Workspace app tried unsuccessfully to contact the connection lease service, `leaseLastCallHomeTi` shows an error with an invalid time stamp:

```
leaseLastCallHomeTime REG_SZ 1/1/0001 12:00:00 AM
```

If `leaseLastCallHomeTime` is uninitialized, the Citrix Workspace app never attempted to contact the connection lease service. To resolve this issue, remove the account from the Citrix Workspace app and add it again.

#### Citrix Workspace app error codes for connection leases

When a service continuity error occurs on the user device, an error code appears in the error message. Common errors include:

| Error code | Description |
|---|---|
| 3000 | No connection lease files present |
| 3002 | Connection lease cannot be read or found |
| 3003 | No resource location found |
| 3004 | Connection details missing in the leases |
| 3005 | ICA file is empty |
| 3006 | Connection lease expired. Log back into store. |
| 3007 | Connection lease is invalid |
| 3008 | Connection lease validation result: empty |
| 3009 | Connection lease validation result: invalid |
| 3010 | Parameter missing |
| 3020 | Connection lease validation failed |
| 3021 | No resource location found where the app is published |
| 3022 | Connection lease validation result: deny |
| 3023 | Citrix Workspace app timed out |
| 3024 | User canceled the lease-based launch while in progress |
| 3025 | Number of launch-retry count exceeded |
| 3026 | Negotiated resource (app or desktop) can not be launched |

#### Access selfservice.txt

To access the `selfservice.txt` file for self-service troubleshooting, perform the following steps:

1. Create a blank text file and name it `enableshieldandlogging.reg`.
2. Copy the following text into the file and save:

```
Windows Registry Editor Version 5.00

[HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\Citrix\Dazzle]
"Tracing"="True"
"AuxTracing"="True"
"DefaultTracingConfiguration"="global all -detail"
"ConnectionLeasingEnabled"="True"

[HKEY_CURRENT_USER\Software\Citrix\Dazzle]
"RemoteDebuggingPort"="8088"
```

3. Place your saved file into your client endpoint.
4. The `selfservice.txt` file is now discoverable at the following path: `%LocalAppData%\Citrix\SelfService`.

#### Troubleshooting for browser users

In the **Advanced** menu of the store account settings, ensure the current method for app and desktop launch preference is set to **Use Citrix Workspace App**. If this option is set to **Use Web Browser**, service continuity isn't supported in the browser.

Ensure that the extension icon in the browser appears green after the browser loads the store URL.

To download logs, click the extension icon in the browser. Then click **Download Logs**.

## Enable single sign-on with Citrix Federated Authentication Service

June 22, 2026

Citrix Federated Authentication Service (FAS) enables single sign-on (SSO) to resources hosted on Active Directory joined VDAs. This ensures that once users have logged on to their store, they can launch virtual apps and desktops without being prompted to re-enter their credentials.

FAS is typically adopted if you're using one of the following identity providers for authentication:

- Microsoft Entra ID

- Okta
- SAML 2.0
- Citrix Gateway
- Google Cloud Identity

FAS isn't needed for SSO to resources if you're using Active Directory (AD), AD plus Token, or specific configurations of Citrix Gateway. For more information on configuring Citrix Gateway, visit Create an OAuth IdP policy on the on-premises Citrix Gateway.

For single sign-on to Entra joined VDAs, instead see Entra ID SSO to VDAs.

## FAS servers

Within each resource location, you can connect multiple FAS servers to Citrix Cloud™ for load balancing and failover purposes.

Citrix Cloud supports using FAS servers in the following scenarios.

In both scenarios, end users signing in to their stores through a federated identity provider enter their credentials only once to access apps and desktops.

### FAS servers connected with a single resource location

If your resource locations contain varied infrastructure (for example, different resource locations contain different AD forests), deploy FAS servers to the resource location where your VDAs are. SSO is active only in resource locations where one or more FAS servers are connected.

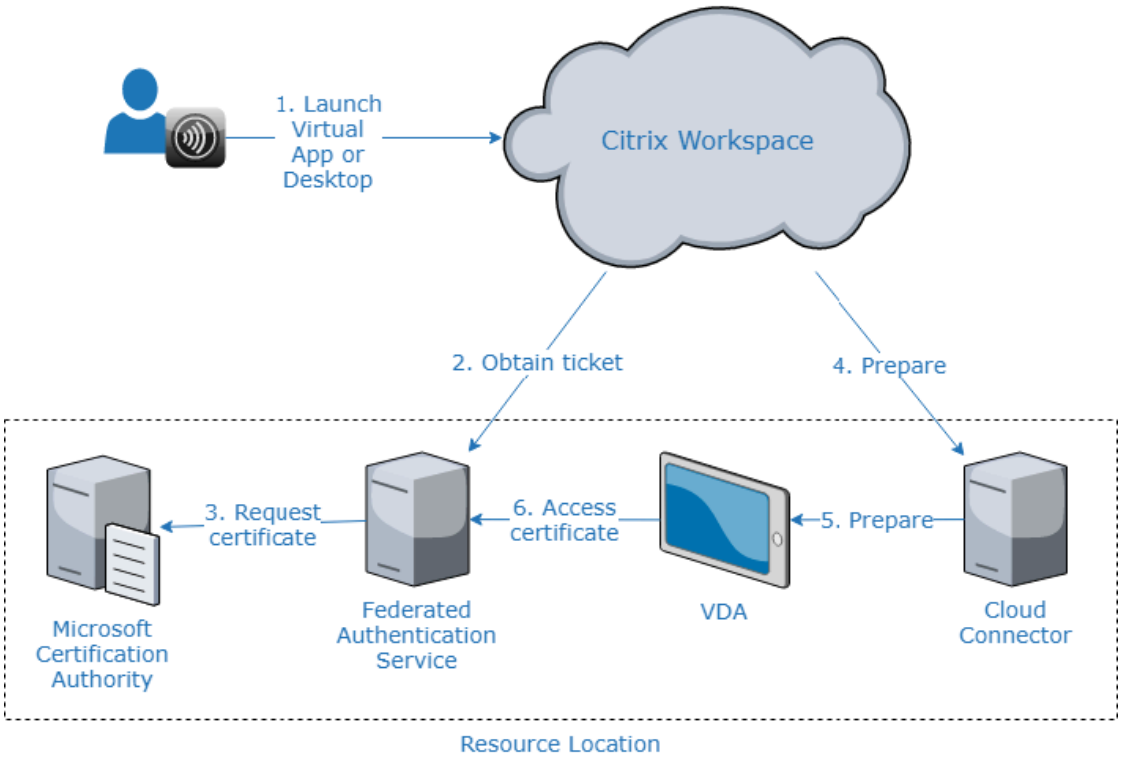
### FAS servers connected with multiple resource locations

If you have network connectivity between your resource locations and they contain similar infrastructure, you can connect your FAS servers with multiple resource locations. SSO is active for store end users who connect to apps and desktops in those resource locations. In this scenario, there's no need to connect separate FAS servers to each resource location.

When end users launch a virtual app or desktop, Citrix Cloud selects a FAS server in the same resource location as the app or desktop that is being launched. Citrix Cloud contacts the selected FAS server to obtain a ticket that grants access to a user certificate stored on the FAS server. To authenticate the end user, the VDA connects to the FAS server and presents the ticket.

You can use the same FAS server for both on-premises and Citrix Cloud with proper rule configuration.




### Failover priority for multiple resource locations

When using FAS servers with multiple resource locations, FAS servers in one resource location can provide failover to FAS servers in other resource locations. When you add FAS servers to other resource locations, you designate each server as primary or secondary. When end users launch a virtual app or desktop, Citrix Cloud uses this designation in the following manner to select a FAS server:

- FAS servers that are designated as primary in the given resource location are considered first.
- If no primary servers are available, FAS servers that are designated as secondary are considered.
- If no secondary servers are available, the launch continues but single sign-on doesn't occur.

### Video overview

For an overview of the Federated Authentication Service for Citrix® StoreFront Cloud, view this Tech Insight video:


## Requirements

### Connectivity requirements

Use the FAS administration console to connect a FAS server to Citrix Cloud. You can use this console to configure a local or remote FAS server. To enable SSO for stores with FAS, the FAS administration console and FAS service access the following addresses using the console user's account and Network Service account, respectively.

- FAS administration console, using the console user's account:
  - `*.cloud.com`
  - `*.citrixworkspacesapi.net`
  - Addresses required by a third party identity provider, if one is used in your environment
- FAS service, using the Network Service account:
  - `*.citrixworkspacesapi.net`
  - `https://*.citrixnetworkapi.net/`

If your environment includes proxy servers, configure the user proxy with the addresses for the FAS administration console. Also, ensure that the address for the Network Service Account is configured as appropriate for your environment.

#### FAS system requirements

You must deploy Federated Authentication Service 2003 (Version 10.1) or later in each of the resource locations where you wish to enable single sign-on. Complete system requirements for the FAS server are described in the System Requirements section of the FAS product documentation.

#### Citrix DaaS™

You must have Citrix DaaS provisioned and enabled in **Service integrations**.

#### Cloud Connectors

Citrix Cloud Connectors enable communication between your resource location (where the VDAs are) and Citrix Cloud. Deploy at least two Cloud Connectors to ensure high availability. The servers on which you install the Cloud Connector software must meet the following requirements:

- System requirements as described in Cloud Connector Technical Details
- No other Citrix components are installed, the server isn't an Active Directory domain controller, and isn't a machine critical to your resource location infrastructure.
- Joined to the domain where your VDAs are.

For more information about deploying Cloud Connectors, refer to the following articles:

- Cloud Connector Proxy and Firewall Configuration
- Cloud Connector Installation

### Setup overview

1. If you're deploying new FAS servers, review the Requirements and follow the instructions in Install and configure FAS in this article.
2. Connect your FAS server to Citrix Cloud as described in Connect a FAS server to Citrix Cloud in this article. Completing this task connects your FAS server to a single resource location.
3. If you plan to connect your FAS server to multiple resource locations, follow the instructions in Add a FAS server to multiple resource locations in this article.

### Install and configure FAS

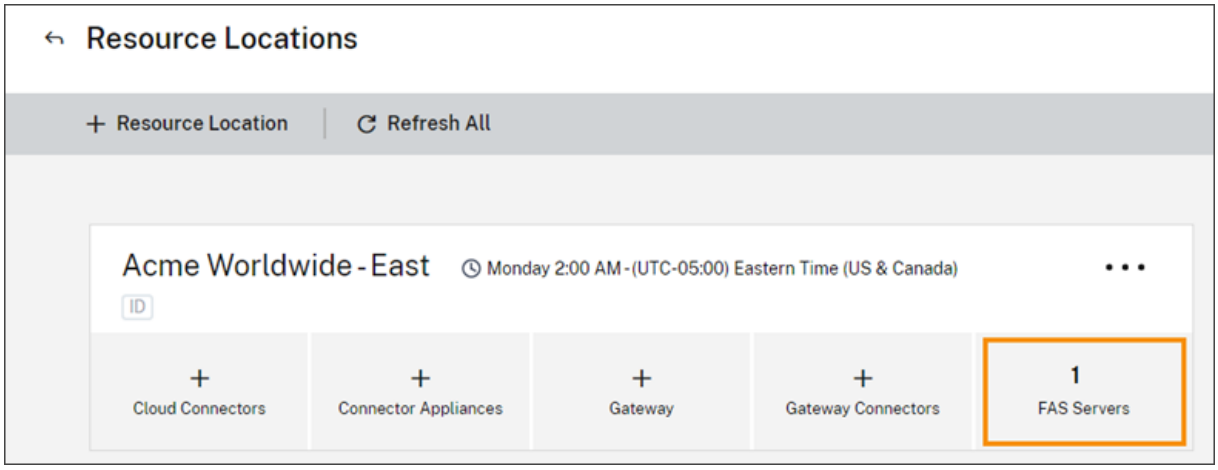
Follow the FAS installation and configuration process described in the FAS product documentation. The configuration steps for StoreFront and the Delivery Controller aren't required.

> **Tip:**
>
> You can also download the Federated Authentication Service installer from the Citrix Cloud console:
>
> 1. From the Citrix Cloud menu, select **Resource Locations**.
> 2. Select the **FAS Servers** tile and then click **Download**.

### Connect FAS servers to Citrix Cloud

Use the FAS administration console to connect your FAS server to Citrix Cloud as described in Install and configure in the FAS product documentation.

After you complete the **Connect to Citrix Cloud** configuration step, Citrix Cloud registers the FAS server and displays it on the Resource Locations page in your Citrix Cloud account.




If you already have the Resource Locations page loaded in your browser, refresh the page to display the registered FAS server.

### Support for Cloud notifications

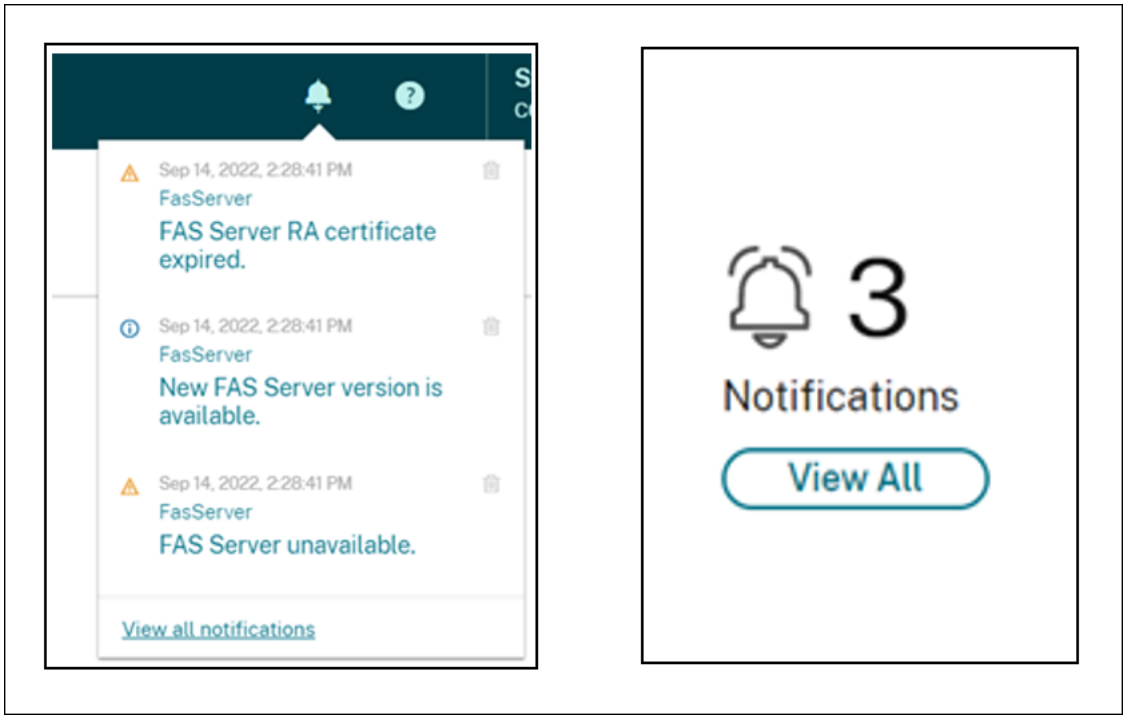
FAS now supports Cloud notifications. With the new Cloud notifications for FAS servers, you receive notifications in the following instances:

- A FAS server is down or unavailable.
- A FAS server's Registry Authority (RA) certificate has expired or is about to expire.
- A new version of FAS is available to download.

### Raising notifications

A periodic check for new notifications is done and raised in the Citrix Cloud management console. The notifications appear under the bell icon on the upper right corner of the Citrix Cloud management console. Select **View All** on the notification icon to view all the notifications. For more information, see Notifications.



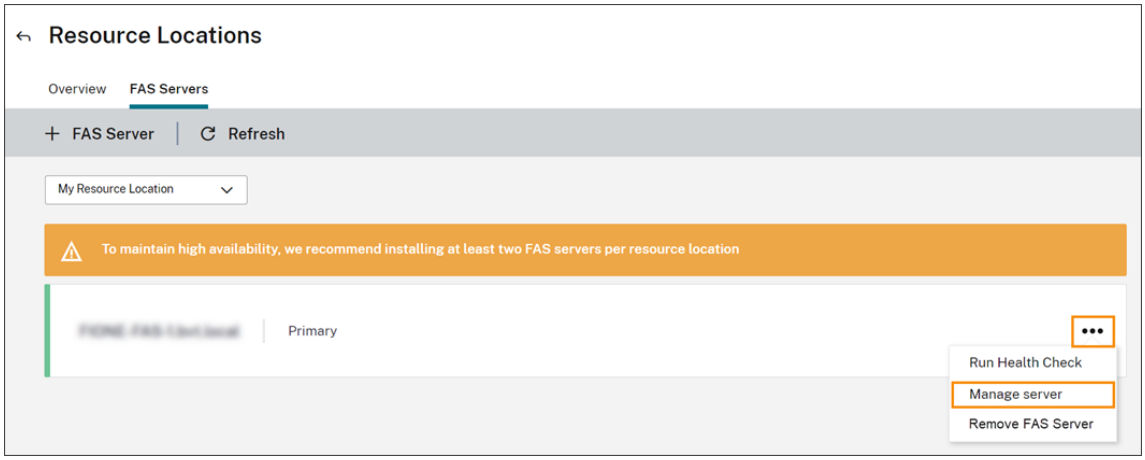

> **Note:**
>
> Once a notification is raised, it will be raised again periodically only if the issue is not resolved.

All notifications contain the FQDN of the impacted FAS server. The RA certificate expiry notification is displayed only for the FAS servers with version 10.10.0.14 and later.

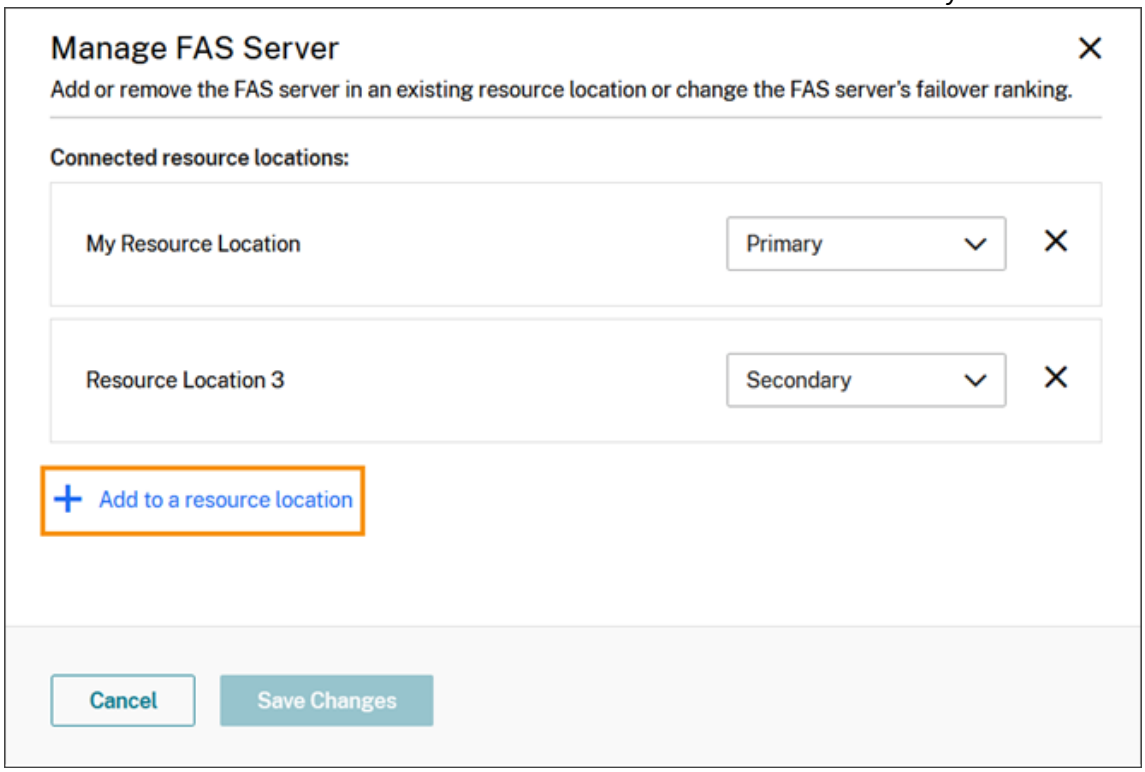
### Add a FAS server to multiple resource locations

1. From the Citrix Cloud menu, select **Resource Locations** and then select the **FAS Servers** tab.
2. Locate the FAS server you want to manage, click the ellipsis (…) at the right side of the entry, and then select **Manage Server**.




3. Select **Add to a resource location** and then select the resource locations that you want.



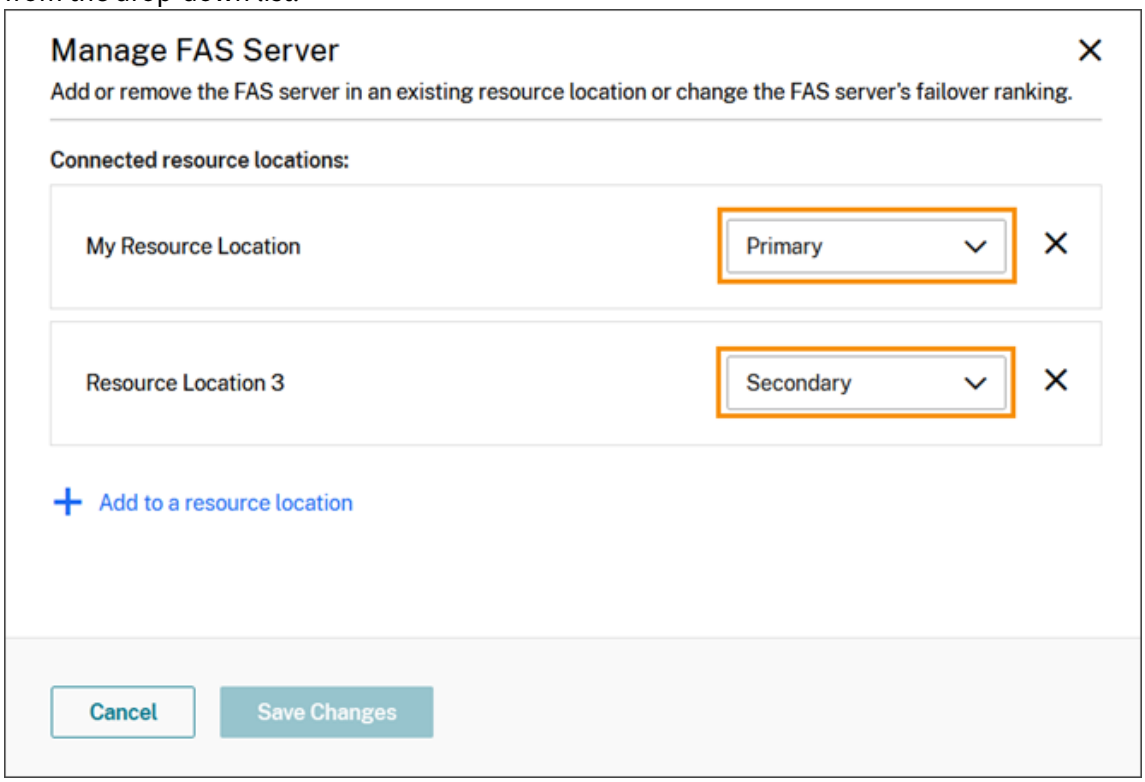

4. Select **Primary** or **Secondary** for the FAS server's failover priority in each selected resource location.
5. Select **Save Changes**.

To view the added FAS server, select **Resource Locations** from the **Citrix Cloud** menu and then select the **FAS Servers** tab. A list of all FAS servers for all connected resource locations appears. To display FAS servers for a specific resource location, select the resource location from the drop-down list.

### Change a FAS server's failover priority

1. From the **Resource Locations** page, select the **FAS Servers** tile for the resource location you want to manage.
2. Select the **FAS Servers** tab.
3. Locate the FAS server you want to manage, click the ellipsis at the right side of the entry, and then select **Manage server**.
4. Locate the resource location with the priority you want to change and select the new priority from the drop-down list.

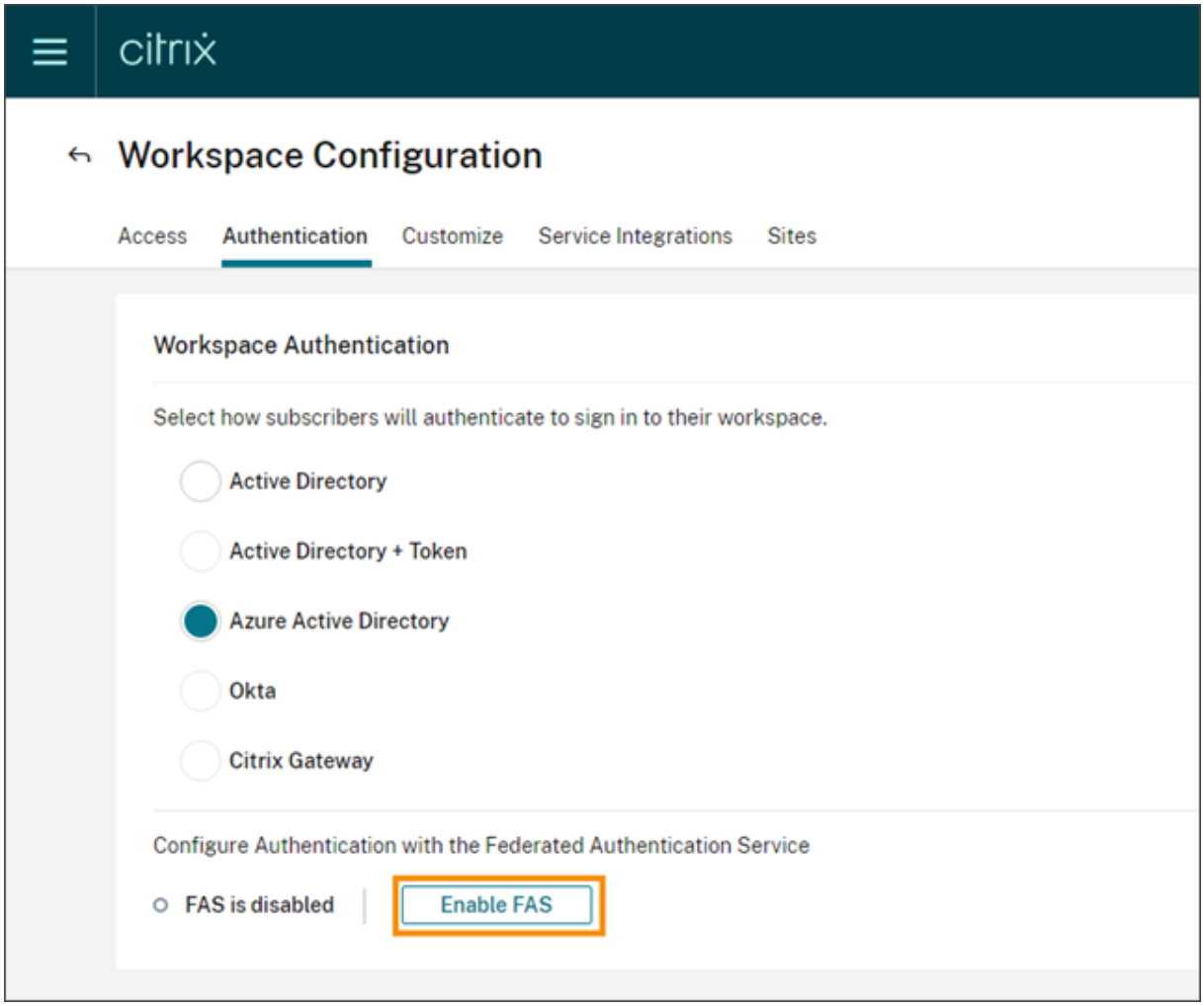



5. Select **Save Changes**.

### Enable federated authentication for stores

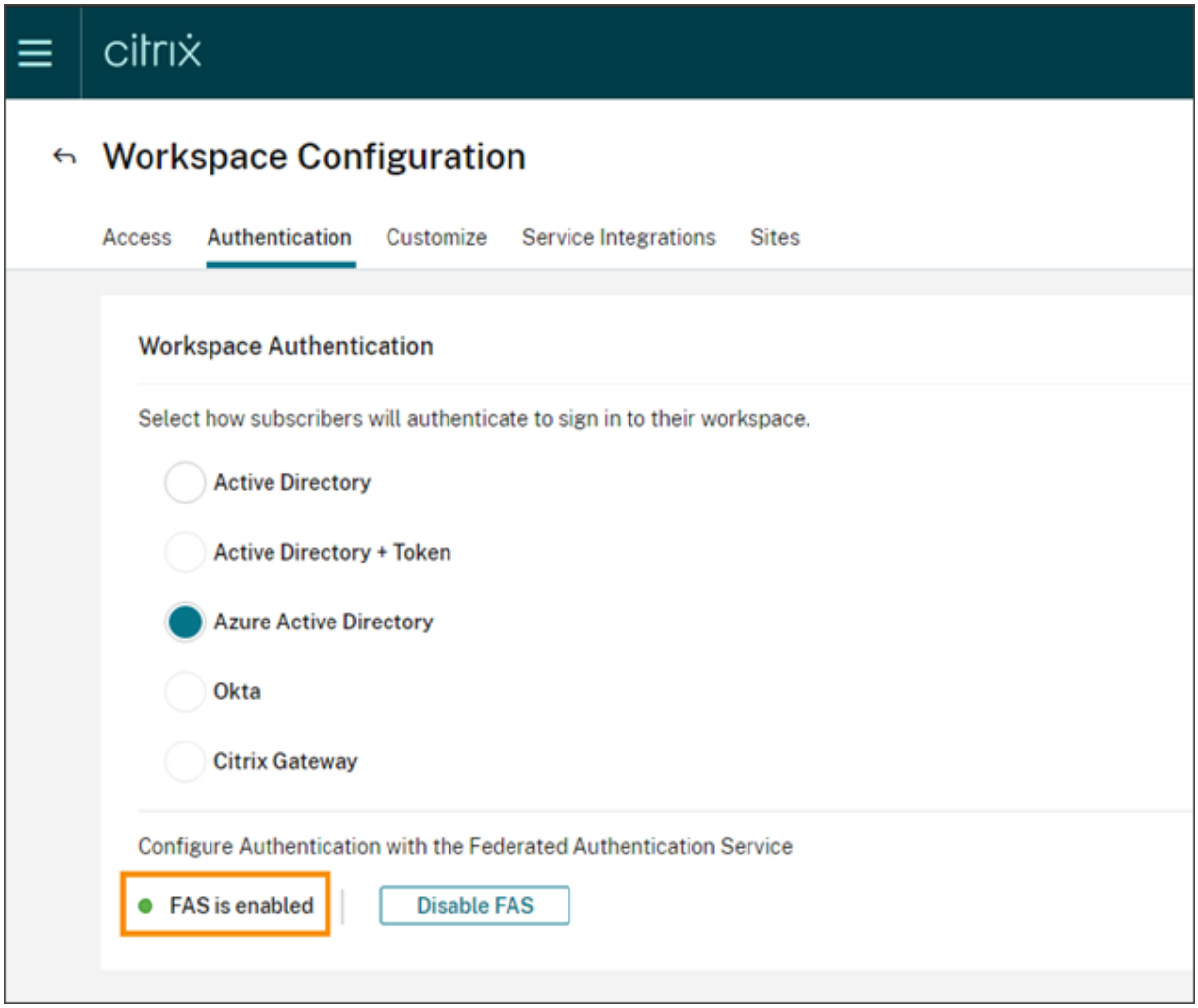
1. From the Citrix Cloud menu, select **StoreFront Cloud** and then select **Authentication**.
2. Click **Enable FAS**. This change might take up to five minutes to be applied to end user sessions.




Afterward, the Federated Authentication Service is active for all virtual app and desktop launches from Citrix® StoreFront Cloud.




When end users sign in to their store and launch a virtual app or desktop in the same resource location as the FAS server, the app or desktop starts without prompting for credentials.

> **Note:**
>
> If all FAS servers in a resource location are down or in maintenance mode, application launches succeed, but single sign-on isn't active. End users are prompted for their AD credentials to access each application or desktop.

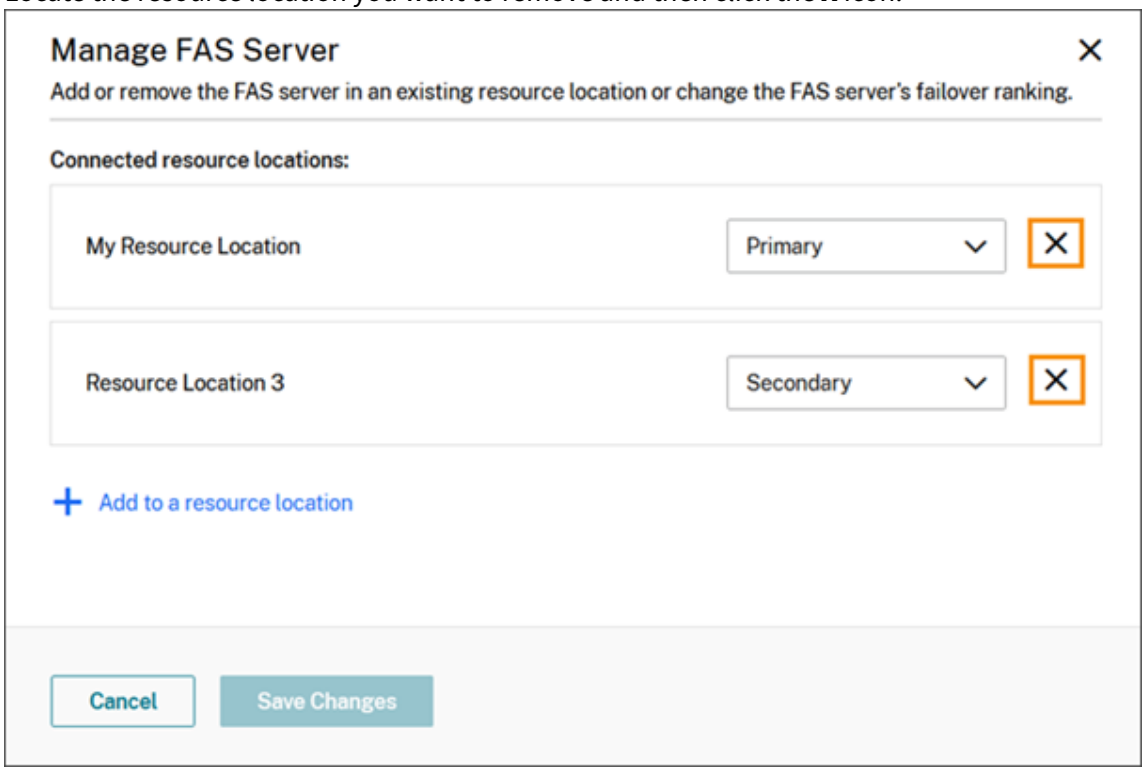
### Remove a FAS server

To remove a FAS server from a single resource location:

1. From the **Resource Locations** page, select the **FAS Servers** tile for the resource location you want to manage.
2. Select the **FAS Servers** tab.

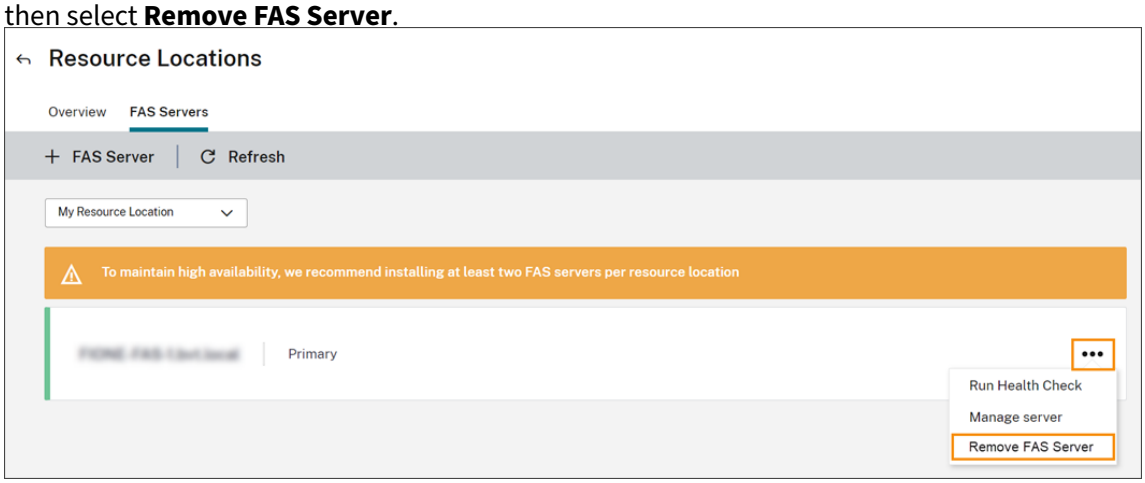
 

3. Locate the FAS server you want to manage, click the ellipsis at the right side of the entry, and then select **Manage server**.
4. Locate the resource location you want to remove and then click the **X** icon.



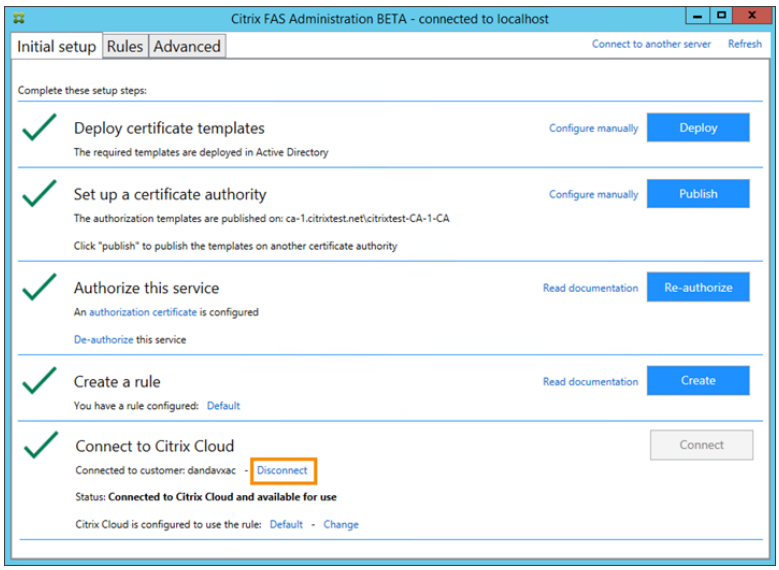

To remove a FAS server from all connected resource locations:

1. From the Citrix Cloud menu, select **Resource Locations**.
2. Locate the resource location you want to manage and then select the **FAS Servers** tile.
3. Locate the FAS server you want to remove, click the ellipsis at the right side of the entry, and then select **Remove FAS Server**.



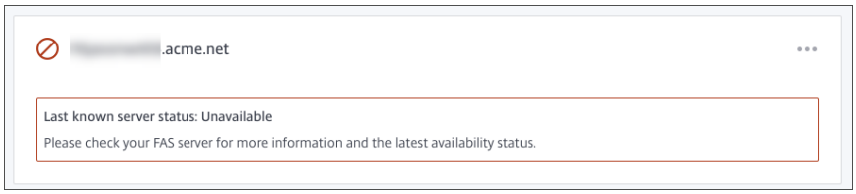

4. On the FAS administration console (on your on-premises FAS server), in **Connect to Citrix Cloud**, select **Disconnect**. Alternatively, you can uninstall FAS.

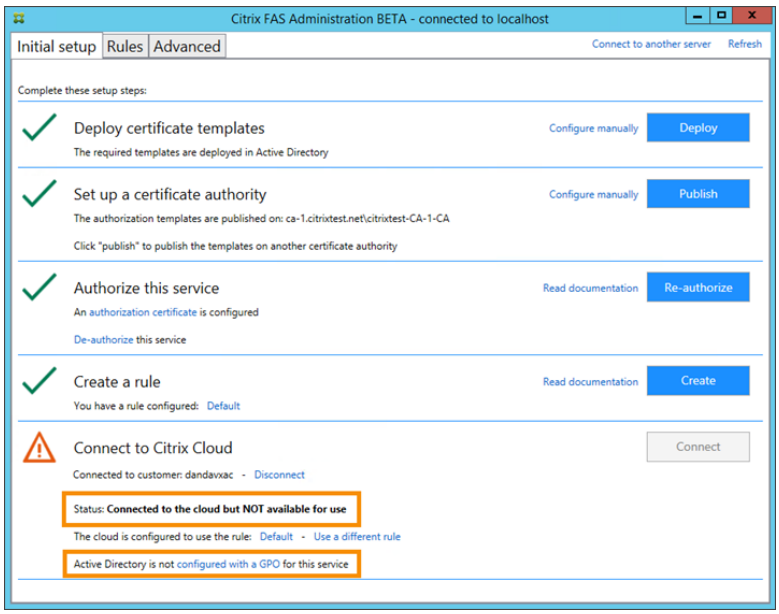



## Troubleshooting

If the FAS server isn't available, a warning message appears on the FAS Servers page.




To diagnose the problem, open the FAS administration console on your on-premises FAS server and inspect the status. For example, the FAS server isn't present in the FAS server GPO:



If the FAS administration console indicates that the server is operating properly, but there are still VDA logon problems, consult the FAS Troubleshooting Guide.

### More information

Configuring Single sign-on to Workspace app

## Resource filtering

June 22, 2026

In Studio you can create resource filters to conditionally hide certain resources based on SmartAccess tags. You can apply resource filters to:

- All resources in a delivery group.
- All resources of a type (app or desktop).
- All resources with a specific tag.

Citrix® StoreFront Cloud generates the following SmartAccess tags that you can include in your filter rules:

| Filter | Value | Description |
|---|---|---|
| Citrix.store.UsingDomain | example.cloud.com | Allows filtering of delivery group resources by store URL. The value is the fully qualified domain name of the `cloud.com` store URL, even when users access store using a custom domain. |
| Citrix-Via-Workspace | True | Indicates that the end user is using Citrix® StoreFront Cloud, rather than an on-premises StoreFront™ deployment. |

These can be used in conjunction with SmartAccess tags from other services such as the user's network location.

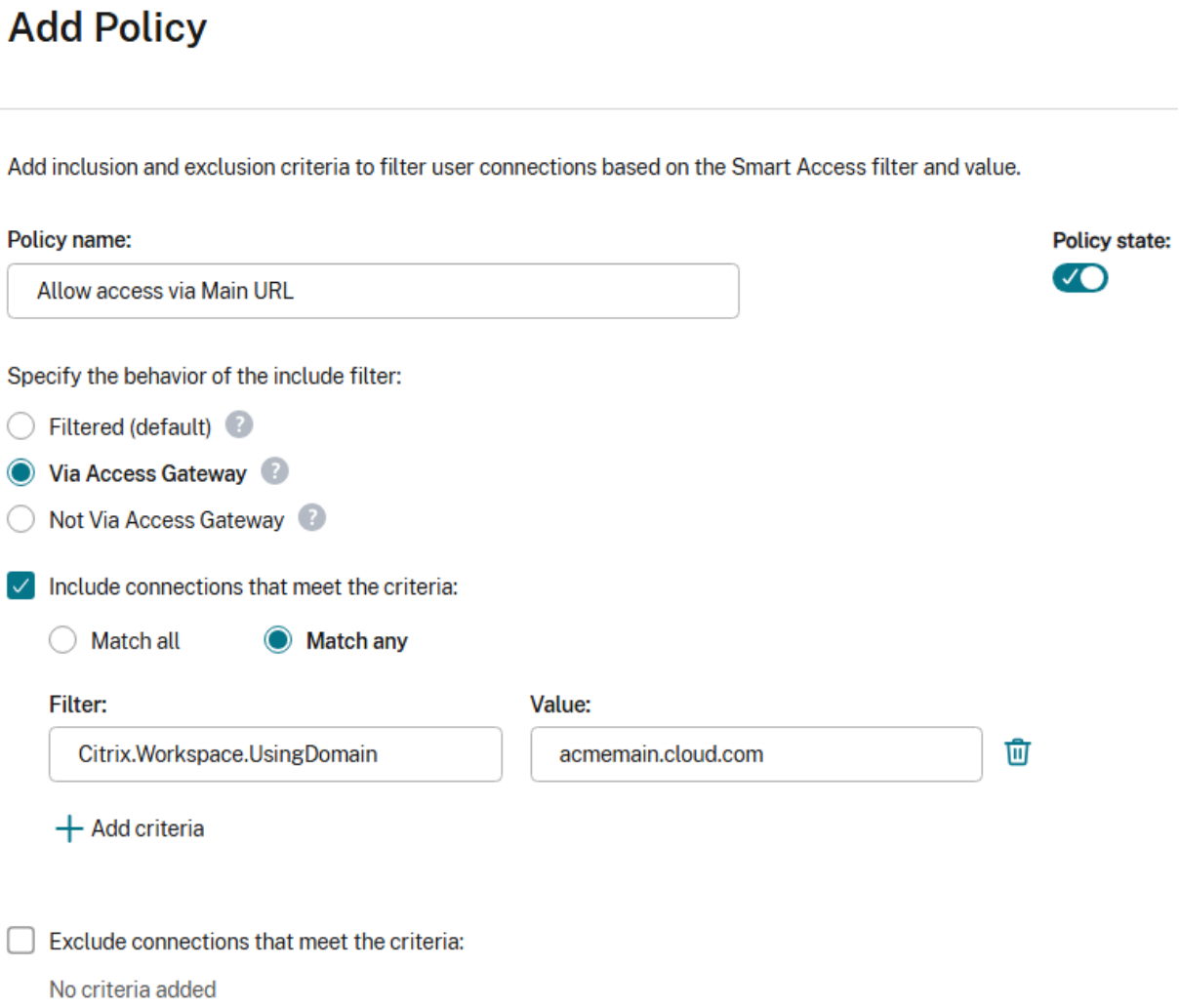
The Delivery Controller™ applies delivery group access policies first, followed by other resource filters. Each filter can remove further resources and cannot reinstate resources that were removed by a previous filter.

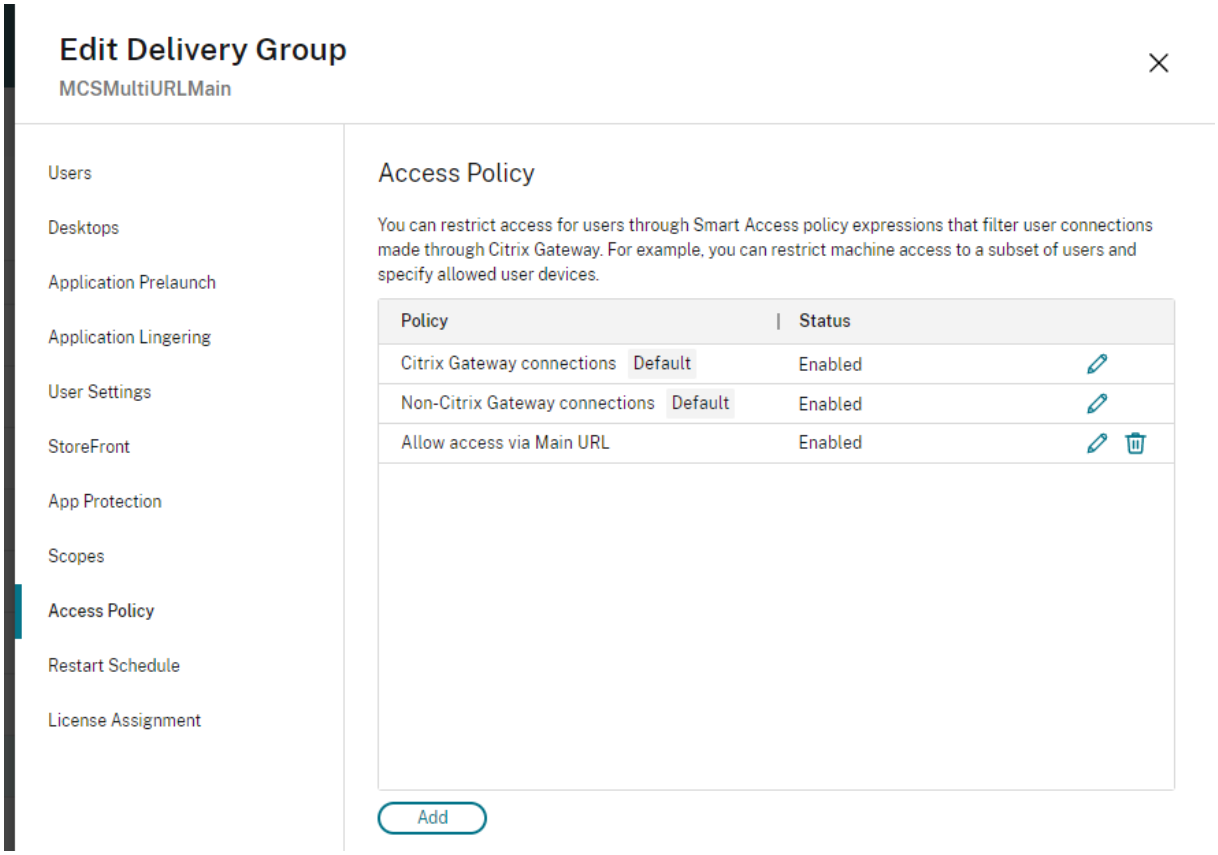
### Apply filters to a delivery group

To apply a resource filter to a Delivery Group, edit the delivery group's **Access policy** to either modify the existing rules or add additional rules. For more information, see Manage delivery groups.

> **Note:**
>
> If Adaptive Access is enabled then DaaS treats requests from Citrix® StoreFront Cloud as being through Citrix Gateway so you must specify the behavior as **Via Access Gateway**. If Adaptive Access is disabled then you specify the behavior as **Not Via Access Gateway**.





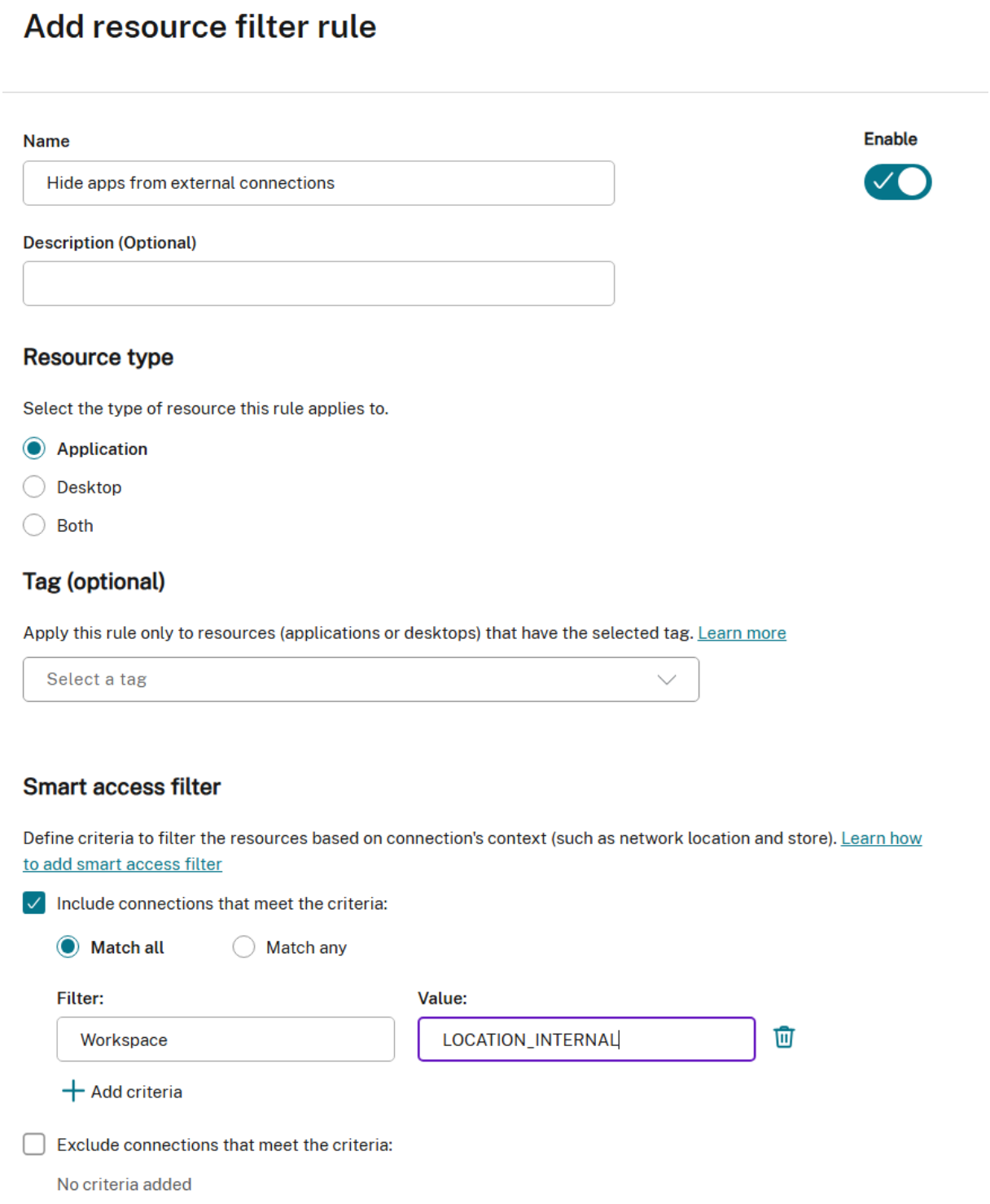

### Apply filters to all resources of a type

To display only resources of a specific type:

1. Add a resource filter with resource type set to **App** or **Desktop**.
2. Enter the **SmartAccess filter** conditions.

For example, to hide all apps from external users




### Apply filters to resources with a tag

If you wish to hide a subset of the apps or desktops within a delivery group, you can do this using Tags.

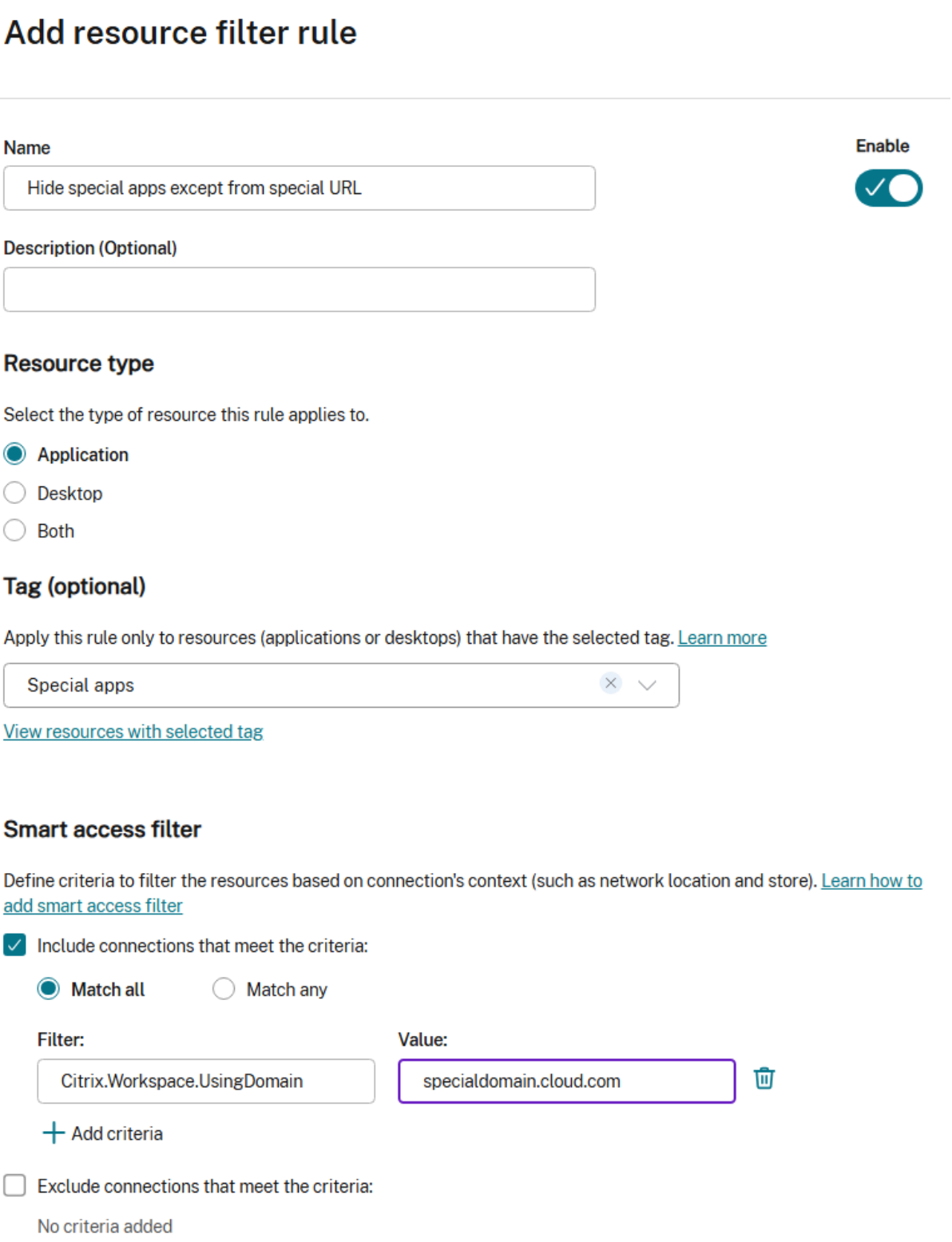
 

> **Note:**
>
> You must tag all of the resources you wish to hide. There is no option to use tags to indicate the resources that you wish to show (i.e. to hide all resources that do not have a specific tag). If you wish to hide newly created resources by default consider using auto tags to automatically tag resources.

1. Apply a **Tag** to the apps and desktops you wish to hide.
2. Create a resource filter applying to that tag.
3. Enter the **SmartAccess filter** conditions.

For example, to hide certain apps except from one specific URL:




To hide the apps from one specific URL, you must have an **Include** rule that covers all URLs, along with an **Exclude** rule for the specific URL for which you wish to hide the resources:

# Add resource filter rule

Name

Hide special apps from special URL

Enable

Description (Optional)

## Resource type

Select the type of resource this rule applies to.

- Application
- Desktop
- Both

## Tag (optional)

Apply this rule only to resources (applications or desktops) that have the selected tag. Learn more

Special apps

View resources with selected tag

## Smart access filter

Define criteria to filter the resources based on connection's context (such as network location and store). Learn how to add smart access filter

Include connections that meet the criteria:

Match all  Match any

Add criteria

Exclude connections that meet the criteria:

Match any

Filter: Citrix.Workspace.UsingDomain

Value: specialdomain.cloud.com

Add criteria

# Configure Citrix Workspace™ app using Global App Configuration service

June 22, 2026

You can configure Citrix Workspace app using Global App Configuration service (GACS). It helps you manage the app settings for end users on both managed and unmanaged devices.
Settings can be configured for both cloud (Citrix® StoreFront Cloud) and on-premises (Citrix StoreFront) environments using one of the following methods:

- Global App Configuration service User Interface (UI):
  - Configure settings for cloud stores
  - Configure settings for on-premises stores
- API: To configure settings using APIs, see Citrix Developer.

This service is supported on Windows, Mac, Linux (cloud store only), Android, iOS, HTML5, and ChromeOS platforms.

## Key benefits

The Global App Configuration service lets you perform the following functions from a centralized interface:

- Configure settings for both managed and unmanaged devices (Bring Your Own Devices)
- Configure settings for multiple stores
- Update and manage client app agents (for example, Endpoint Analysis, ZTNA) and third-party agents (for example, Zoom, Webex)
- Automatically update and manage the Citrix Workspace app version for end users
- Test the configuration before rolling it out to your end-users

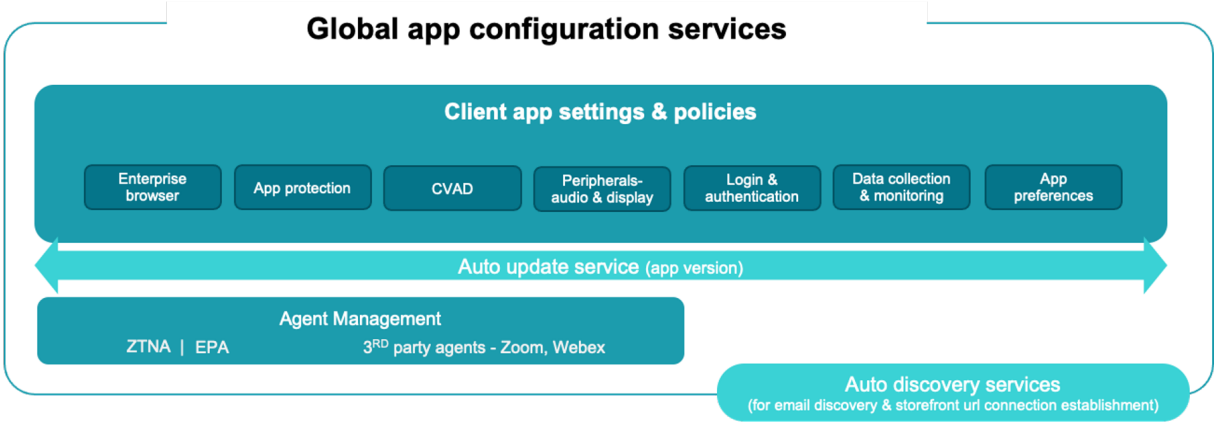
## How does the Global App Configuration service work?

The Global App Configuration service is a Citrix IP solution used to configure and manage client app settings. It uses the following services and settings to provide a seamless experience to your end-users.

- **AutoDiscovery services**: It maps domains to store URLs, enabling your end users to sign in using their email addresses. End users aren't required to provide their store URLs at the time of sign-in.

- **Auto-update service and Agent management**: Automatically updates Citrix Workspace app to the specified version for your end users. You have the flexibility to configure different app versions for different platforms.
- **Client app settings and policies**: All end-user settings on Citrix Workspace app can be configured and set centrally. It includes settings such as login experience, security, authentication options, virtual app, desktop settings.




> **Note:**
>
> With the release of Citrix Workspace app version 2402 for Windows and Mac, GACS serves settings in two stages. Citrix Workspace app initially fetches certain settings that need to be applied before user authentication, and the rest of the settings are applied after the successful authentication.

### Prerequisites

Before you configure the app settings, verify that the Citrix Workspace app version is equal to or higher than the specified versions. For more information, refer to the following table.

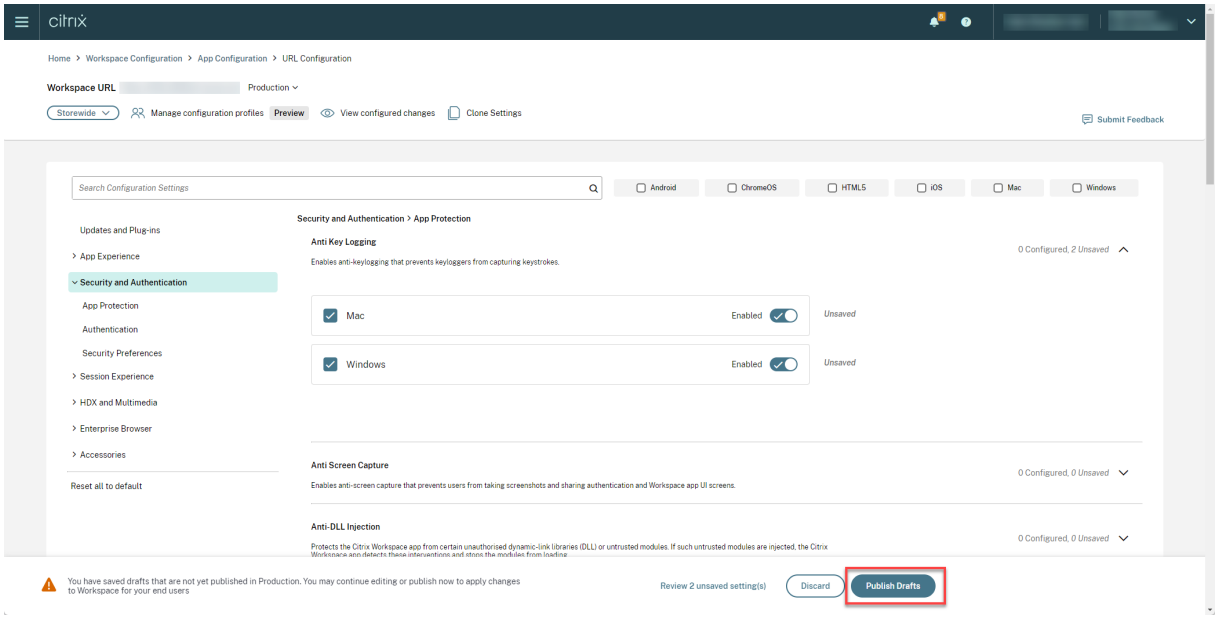
| Citrix Workspace app platform | Minimum supported version |
|---|---|
| Windows | Current Release - 2106, LTSR - 2203.1 |
| Mac | 2203.1 |
| Linux | 2408 |
| iOS | 2104 |
| HTML5 | 2111 |
| ChromeOS | 2203 |
| Android | 2104 |

### How to use the Global App Configuration service?

To configure settings:

1. Sign in the Citrix Cloud portal and navigate to **StoreFront Cloud** > **App configuration**.
2. From the list of configured store URLs, select the store for which you want to map settings and then click **Configure**.
3. Modify the app settings as per your organization's policies.
4. Click **Publish Drafts** to save and publish your settings.

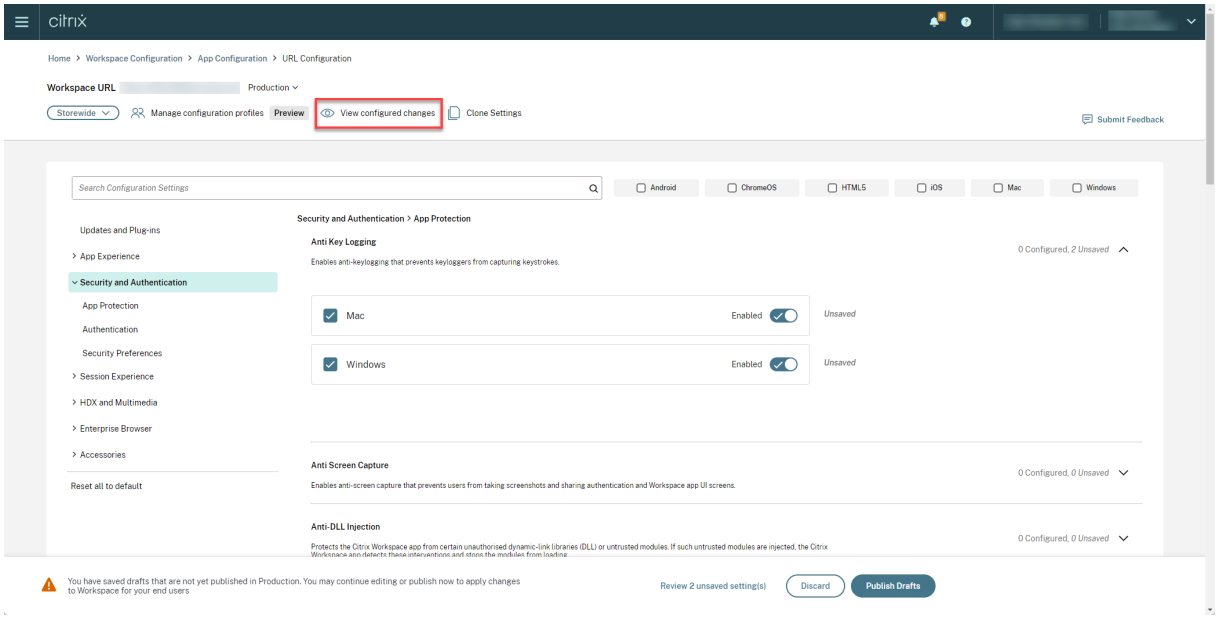



The user interface also provides the following options for a simplified user experience.

### View a summary of configured settings

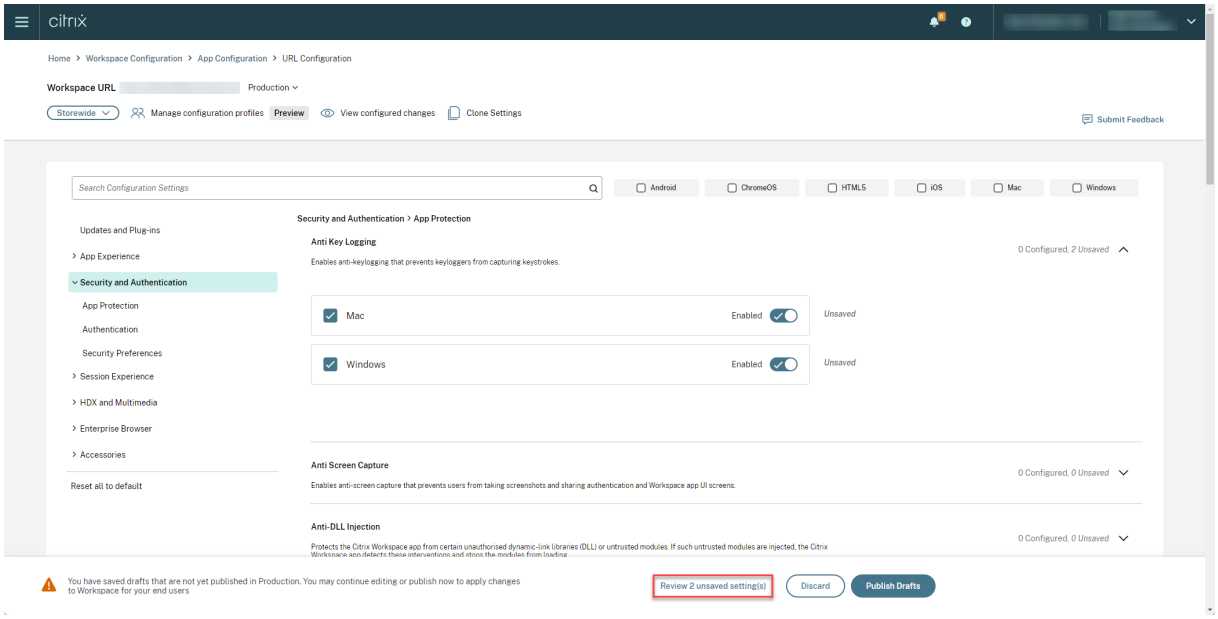
You can view a summary of the current configuration by clicking the **View configured changes** button. It eliminates the need to expand and review each setting separately. A consolidated list of all the configured settings allows you to perform a comprehensive review of the current configuration and gauge the user impact.



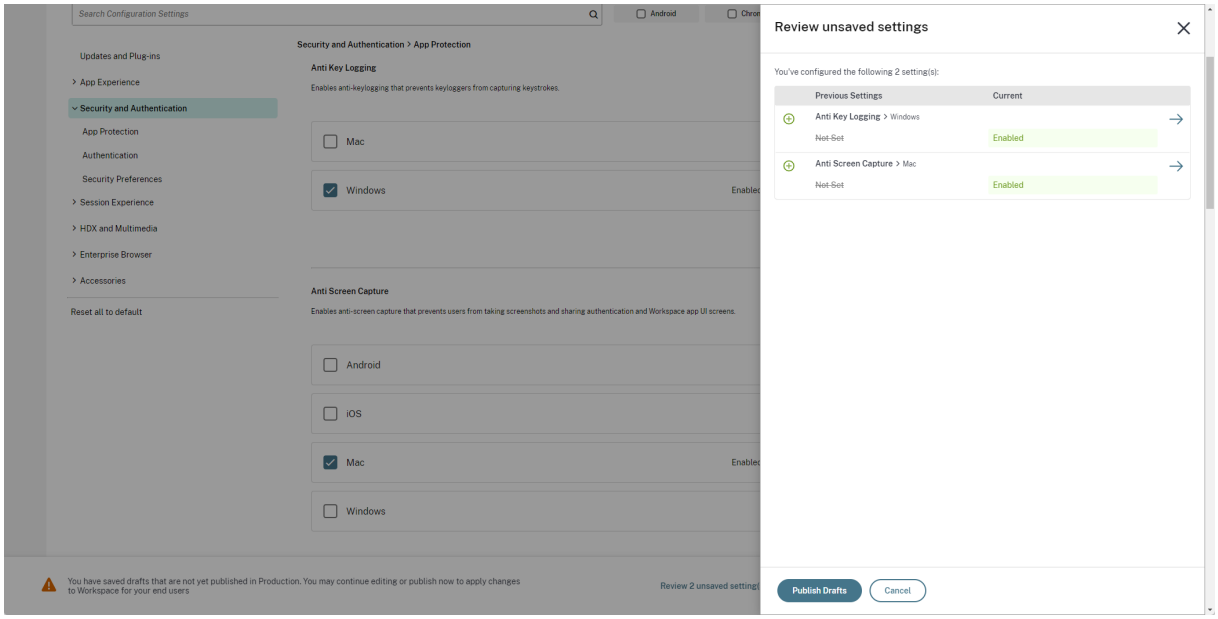

## Review unsaved changes

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.




You can also navigate to an unsaved setting by clicking the arrow.

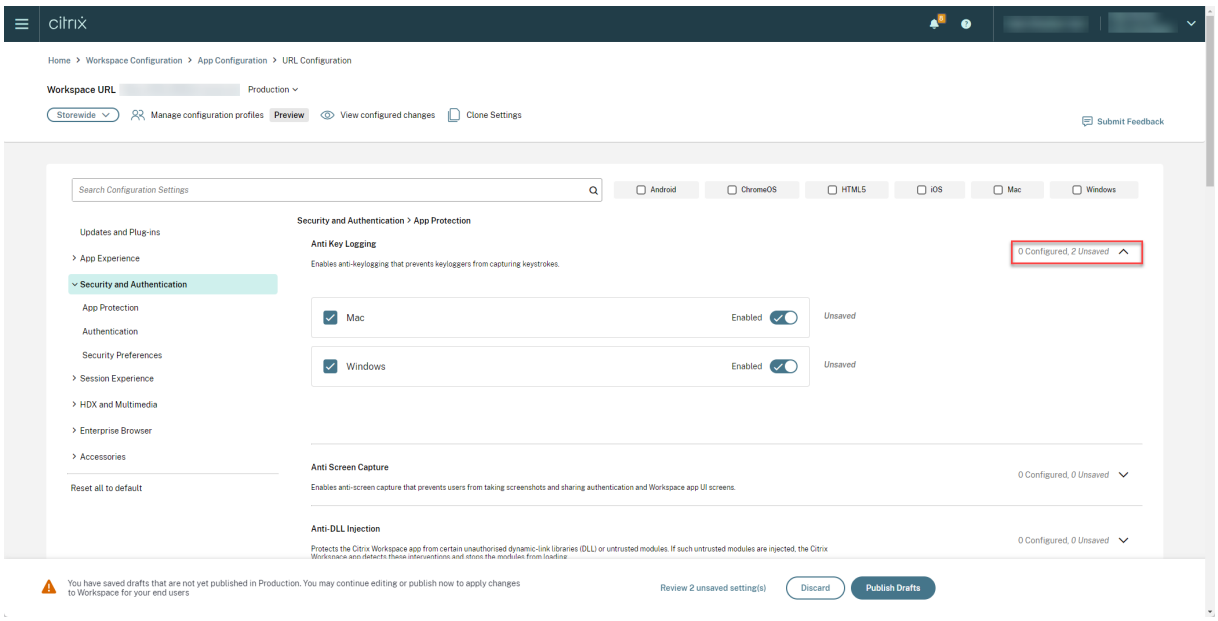
 




### Enhanced user interface

View the status of each setting without expanding it. The following tags are now displayed to facilitate informed decision making at every step.

- **Configured**: Displays the number of platforms (client OS) for which the setting has already been configured.
- **Unsaved**: Displays the number of settings that are configured but not yet saved



### 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 App Configuration page with ease. They can use the following search methods.

- **Search using setting description**

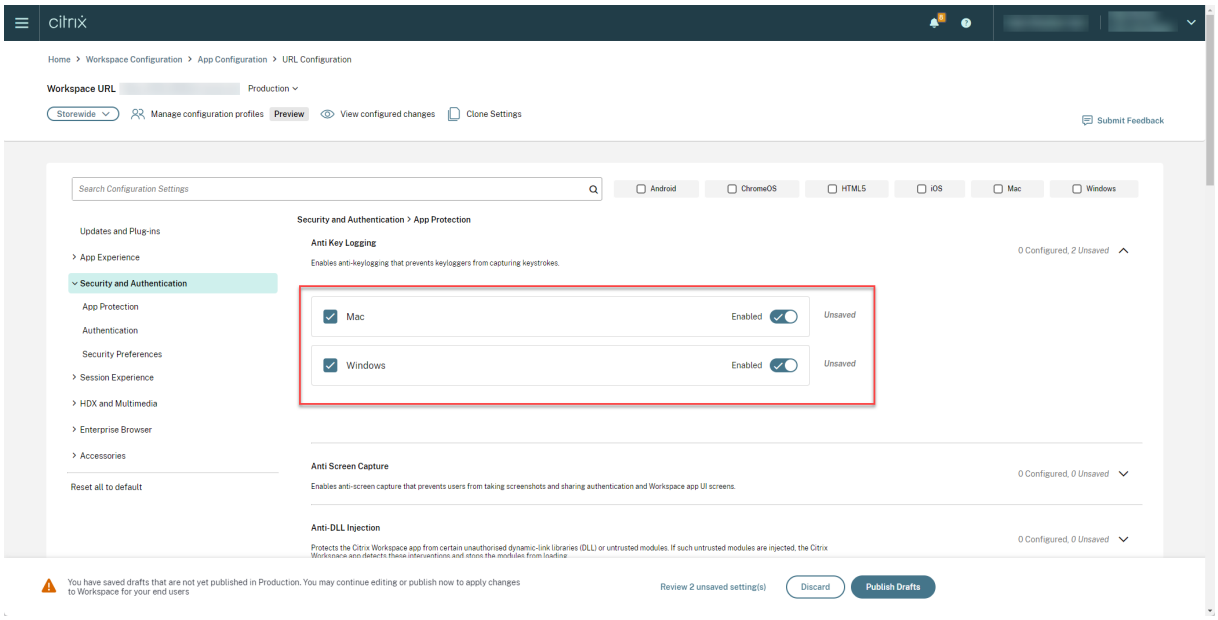
You can locate settings by entering keywords found within the setting's description. It allows for a more flexible search approach, using relevant terms associated with the desired setting.

- **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.




### Frequency of fetching updated settings

Once the configuration is published, it might take a few hours for the settings to be updated on the client side.

- In the same session, settings are updated as follows.

| Platform | Maximum time required to update settings |
|---|---|
| Citrix Workspace app for Windows | up to 6 hours |
| Citrix Workspace app for macOS | up to 6 hours |
| Citrix Workspace app for Linux | up to 6 hours |
| Citrix Workspace app for HTML5 | up to 3 hours |
| Citrix Workspace app for ChromeOS | up to 3 hours |
| Citrix Workspace app for iOS | up to 6 hours |
| Citrix Workspace app for Android | up to 6 hours |

- For Windows and macOS, settings can be updated immediately if the end users exit and restart their Citrix Workspace app.
- When an end user adds a store to their Citrix Workspace app, the settings for that store are updated automatically.

### Order of precedence for application of settings

In addition to the Global App Configuration service, there are platform specific tools, such as GPO for Windows, that can be used to configure end-user settings.
In the event of a conflict between settings configured through the Global App Configuration service 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 Cloud | **Group Policy Object (GPO) or MDM > Global App Configuration service** |
| Citrix Workspace app for Mac | StoreFront and Cloud | **MDM > Global App Configuration service > UserDefaults** |
| Citrix Workspace app for Linux | Cloud | **MDM > Global App Configuration service** |
| Citrix Workspace app for HTML5 | StoreFront | Global App Configuration service > Configuration.js |

| Platform | Store type | Order of precedence |
|---|---|---|
| | Cloud | Global App Configuration service |
| Citrix Workspace app for ChromeOS | StoreFront | **Google Admin Policy > Global App Configuration service >** Configuration.js |
| | Cloud | **Google Admin Policy > Global App Configuration service** |
| Citrix Workspace app for iOS | StoreFront and Cloud | Global App Configuration service |
| Citrix Workspace app for Android | StoreFront and Cloud | Global App Configuration service |

### Limitations

Only the first Global App Configuration service-enabled store can fetch the setting.

### Additional Resources

- Technical Brief on Global App Configuration service
- FAQs: Global App Configuration service settings and behaviors
- Webinar recording: How to use Global App Configuration service
- Citrix Features Explained: Global App Configuration Service

## What's new in Global App Configuration service

September 16, 2025

The following sections list the new features in current and earlier releases for the Global App Configuration service.

## Aug 06, 2025

### GACS supports hybrid launch

Starting with version 2503, Citrix Workspace™ app for Windows and Mac enables its management via Global App Configuration service (GACS) for hybrid launch.

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 opening 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, GACS 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.

To learn more about the feature, see Manage settings for hybrid launch.

## July 08, 2025

### Configure settings for custom domain

The Global App Configuration service (GACS) allows you to assign settings to both *custom domains* and the *cloud.com domain*. Administrators can configure a custom domain for their default Workspace URL, and the settings applied to that Workspace URL extends to the linked custom domain.

For more information, see Configure settings for custom domain.

## May 09, 2025

### 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 Global App Configuration service, you can manage the ControlUp's RemoteDX Plug-in manager.

For more information, see ControlUp's RemoteDX Plug-in Management.

## Apr 03, 2025

### GACS supports hybrid launch (Technical Preview)

Starting with version 2503, Citrix Workspace app for Windows and Mac enables its management via Global App Configuration service (GACS) for hybrid launch.

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 opening 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, GACS 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.

To learn more about the feature, see Manage settings for hybrid launch.

## Dec 20, 2024

### Configuration profile feature is available for on-premises store users

The configuration profiles feature in Global App Configuration service allows the administrators to configure settings for user groups. This feature is now available for on-premises stores as well. For more information on compatible Citrix Workspace app versions that support this feature, see Verify Citrix Workspace app version.

For more information, see Manage settings for user group using configuration profiles.

## Dec 12, 2024

### Define timeframe for automatic update

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.

For more information, see Automatic update timeframe.

### Manage automatic update version and rollout period for Citrix Workspace app

Administrators can schedule convenient date ranges during which an automatic update of Citrix Workspace app should roll out to their end users. This capability allows them to determine the rollout dates, minimizing disruption to end users and improving the user experience.

For more information, see Citrix Workspace app version.

### Automatic update management settings supports configuration profiles

The automatic update management settings such as **Automatic update timeframe** and **Citrix Workspace app version** are applicable for different user groups through configuration profiles.

For more information, see Automatic update management settings supports configuration profiles.

### Oct 09, 2024

#### Configuration profile feature is available on Linux and Android for cloud store users

The configuration profiles feature in Global App Configuration service allows the administrators to configure settings for user groups. Starting with the release of Citrix Workspace app version 2408 for Linux and version 24.9.0 for Android, this feature is available on Linux and Android for cloud store users.

For more information, see Release note: Citrix Workspace app for Linux and Release note: Citrix Workspace app for Android

Learn more about the feature in Manage settings for user group using configuration profile.

### Sep 24, 2024

#### Configuration profile feature is available on iOS for cloud store users

The configuration profiles feature in Global App Configuration service allows the administrators to configure settings for user groups. Starting with the release of Citrix Workspace app version 24.9.0 for iOS, this feature is available on iOS for cloud store users.

For more information, see Release note: Citrix Workspace app for iOS

Learn more about the feature in Manage settings for user group using configuration profile.

### Jul 02, 2024

#### Plug-in Manager is available for Microsoft Teams

Starting with Citrix Workspace app for Windows version 2405, administrators can now optimize the audio and video for calls and meetings using the Microsoft Teams VDI plug-in manager. This enhancement provides improved performance and user experience during virtual meetings. The installation and configuration of the Microsoft Teams VDI plug-in manager can be managed through the Global App Configuration service. This Plug-in Manager, in turn, installs and manages the Microsoft Teams Optimization plug-in (VDI 2.0 or Slimcore engine) on the end-user's device.

For more information, see Microsoft Teams VDI Plug-in Management.

## Jun 04, 2024

### Clone settings across stores, channels, and configuration profiles

Administrators can now clone settings across stores, channels, and configuration profiles through Global App Configuration service using a new feature called **Clone Settings**. This feature allows you to duplicate existing settings instead of going through the entire configuration process again. Consequently, it saves a lot of time and effort, resulting in better productivity and streamlined workflows.

For more information on configuring this feature, see Clone settings across stores, channels, and configuration profiles.

## May 29, 2024

### Applying GACS settings on first-time use of Citrix Workspace app for HTML5

Starting with Citrix Workspace app for HTML5 version 2404.1 and later, Global App Configuration service (GACS) settings are applied when end users start a Workspace session for the first time. End users might also be prompted to restart their session to ensure compliance.

For more information, see Citrix Workspace app for HTML5 product documentation.

## May 07, 2024

### Manage settings for user groups using configuration profile (Preview)

With the release of Citrix Workspace app version 2402 for Mac and Windows, you now can manage settings for user groups using **Configuration profile** in Global App Configuration service (GACS). A configuration profile is used to identify a collection of user groups. It allows you to manage settings for user groups rather than applying them to all users accessing the store. To do so, you can create a configuration profile and add the desired user groups to it. You can then choose the configuration profile, assign settings, and publish them to apply specific experiences to different user groups..

For more information on configuring settings for configuration profile , see Manage settings for user group using configuration profile.

> **Note:**
>
> This feature is currently applicable for cloud stores on the Windows and Mac platforms. The support for other platforms will soon be available.

## Apr 11, 2024

### Improvements in Global App Configuration service

With the release of Citrix Workspace app version 2402 for Windows and Mac, we have enhanced Global App Configuration service (GACS) in the following areas:

**Settings are secured with user authentication** GACS now serves settings in two stages. Citrix Workspace app initially fetches certain settings that need to be applied before user authentication, and the rest of the settings are applied after the successful authentication.

This capability paves the way for an upcoming GACS feature that gives you the ability to configure settings for a user based on the user group to which that user belongs.

> **Note:**
>
> The authenticated GACS is currently available only for Workspace stores. The support for StoreFront stores will soon be available.

**Discovery improvements** Citrix Workspace app now has the improved ability to discover and configure settings for various user inputs. Users can now start using the app with either an email address, domain name or store URL. Based on the user input, GACS discovers the associated store URLs and adds all of them.

Previously, when you map multiple store URLs to a domain and configure GACS settings for more than one of the store URLs, users were unable to add any store to Citrix Workspace app because it discovers multiple stores. However, starting with the 2402 release, this limitation is removed.

> **Note:**
>
> Starting with Citrix workspace app for Windows 2402 and Mac 2402, you can add more than one GACS-enabled store. The store that you add first takes the precedence in assigning value to the settings, and subsequent stores inherit the behavior determined by the first store. In the upcoming release, we're introducing a setting for administrators that allows you to manage whether a store can be added to Citrix Workspace app as a single store or as part of multiple stores. In the meantime, if you wish to enable this setting, contact Citrix Support.

**Full StoreFront URL support** GACS has the added flexibility to configure different settings for StoreFront URLs with a common FQDN. Let's take the examples of the stores `https://mywork.acme.com/Citrix/StoreFTE` and `https://mywork.acme.com/Citrix/StorePartner`. Previously, you could configure settings only at `https://mywork.acme.com` (FQDN) level, which didn't provide the flexibility to configure different settings for each of the stores: `StoreFTE` and `StorePartner`.

## Mar 18, 2024

### Additional settings for Citrix Enterprise Browser™

Global App Configuration service (GACS) has new settings to configure Citrix Enterprise Browser that allow you to manage the following actions:

- Autofill suggestions for the addresses
- Autofill suggestions for credit card information
- Launch an external application without prompting the user
- Display the security warnings when potentially dangerous command-line flags are used to launch the browser.
- Manage the default cookie setting
- Manage the default pop-up setting
- Install the extensions, apps, and themes to the browser
- Suppress the warnings for any suspected lookalike domains in the browser
- Allows the websites to check saved payment methods
- Manage the saving of the browser history
- Manage the search suggestion in the browser's address bar
- Export a bookmark
- Create an ephemeral profile when users sign in to the Enterprise Browser

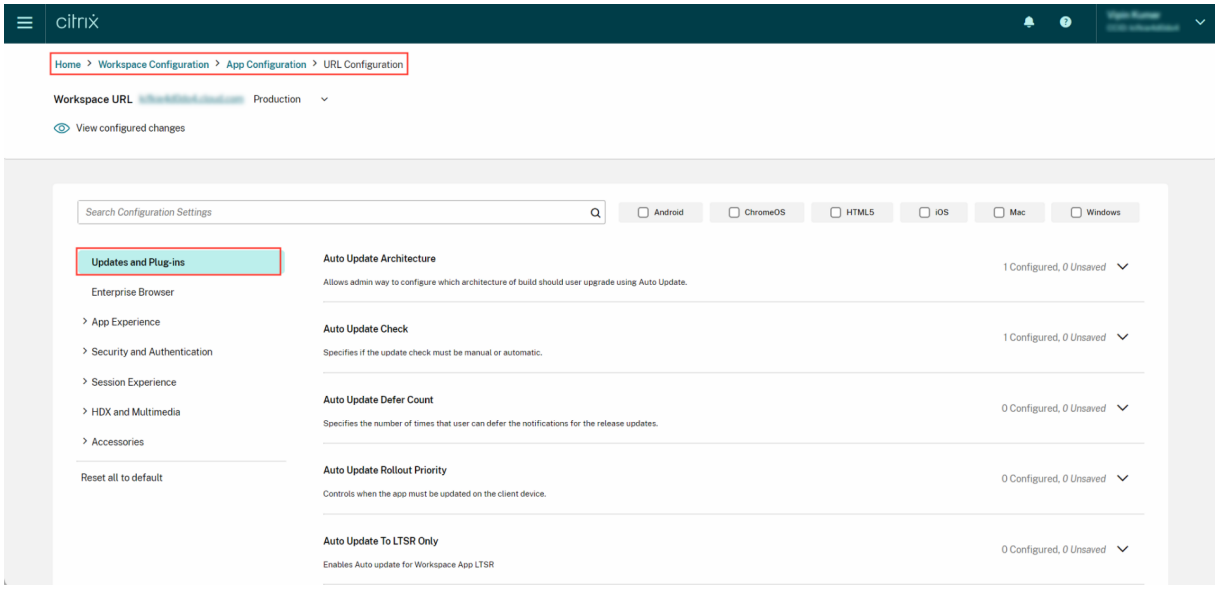
For more information about the settings, see Manage Citrix Enterprise Browser through Global App Configuration service in the Citrix Enterprise Browser product documentation.

## Jan 18, 2024

### Manage plug-ins using Global App Configuration service

The Global App Configuration service provides a centralized platform that helps you configure installation and update settings for plug-ins. You can distribute plug-in settings across both managed and unmanaged devices. To configure plug-in settings, navigate to the **Updates and Plug-ins** category under **Workspace Configuration** > **App Configuration** on the cloud portal. For more information, see Plug-in management.




You can configure the following plug-ins:

- Citrix Endpoint Analysis Plug-in
- Citrix Secure Access Agent
- Webex VDI AutoUpgrade Plug-in
- Zoom VDI Plug-in Management

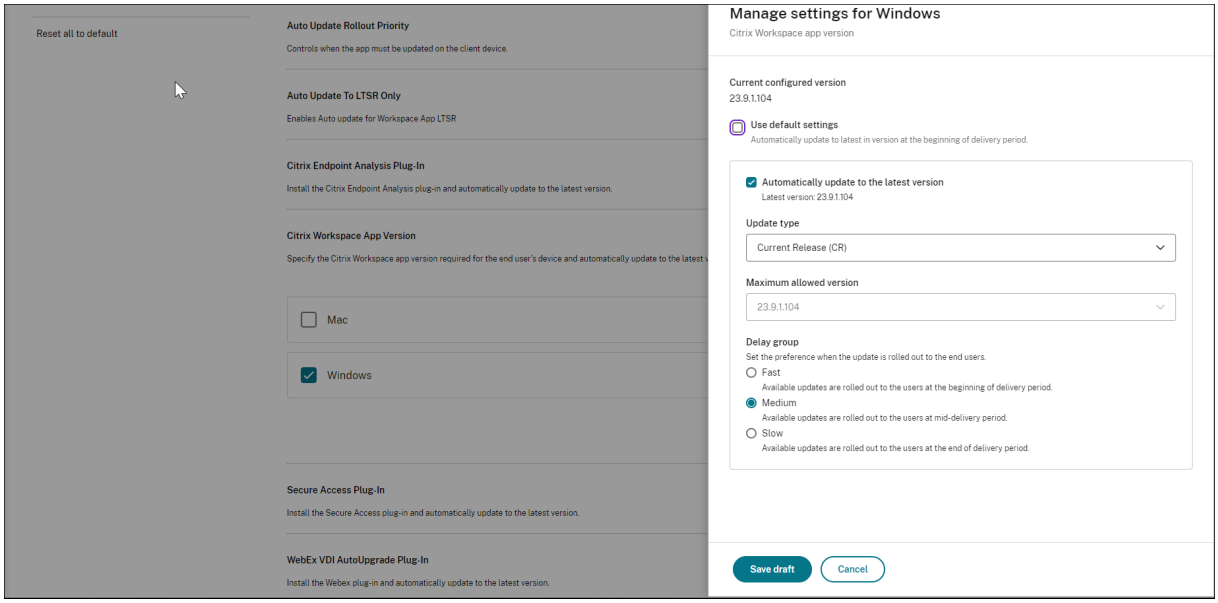
## Nov 21, 2023

### Manage Citrix Workspace app version

As an admin, you can now manage auto-update or version settings for Citrix Workspace app from a centralized platform. You can customize your settings for both **CR** (Current Release) and **LTSR** (Long Term Service Release) versions. You can set up a rule that updates your end users automatically to the latest version, whenever a new version is available. If you do not want to update to the latest version, you can also specify a preferred version that the end users must update to for optimal results.

The **Citrix Workspace App Version** setting can be customized for Windows and Mac platforms from the **Updates and Plug-Ins** section. For more information, see Manage Citrix Workspace app versions.




## Oct 30, 2023

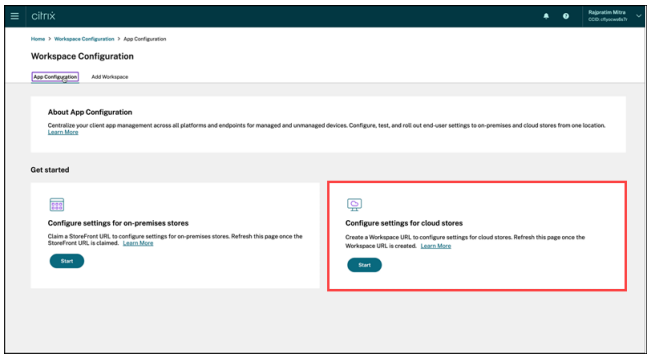
### Configure settings for on-premises stores

You can now use the Global App Configuration service UI to configure settings for on-premises stores. Sign in to your Citrix Cloud™ account and navigate to **Workspace Configuration > App Configuration** to get started.

> **Note:**
>
> If you don't have a Citrix Cloud account yet, go to the Citrix Onboarding page to create one.

Before proceeding, verify that you've established a claim to your StoreFront URL. If you've claimed your StoreFront URL, see the Configure settings section for more information.

If you haven't claimed your StoreFront URL yet, you can claim it. For that, click **Claim URL** under the **App Configuration** section to claim your URL. For more information, see Get started with configuration.

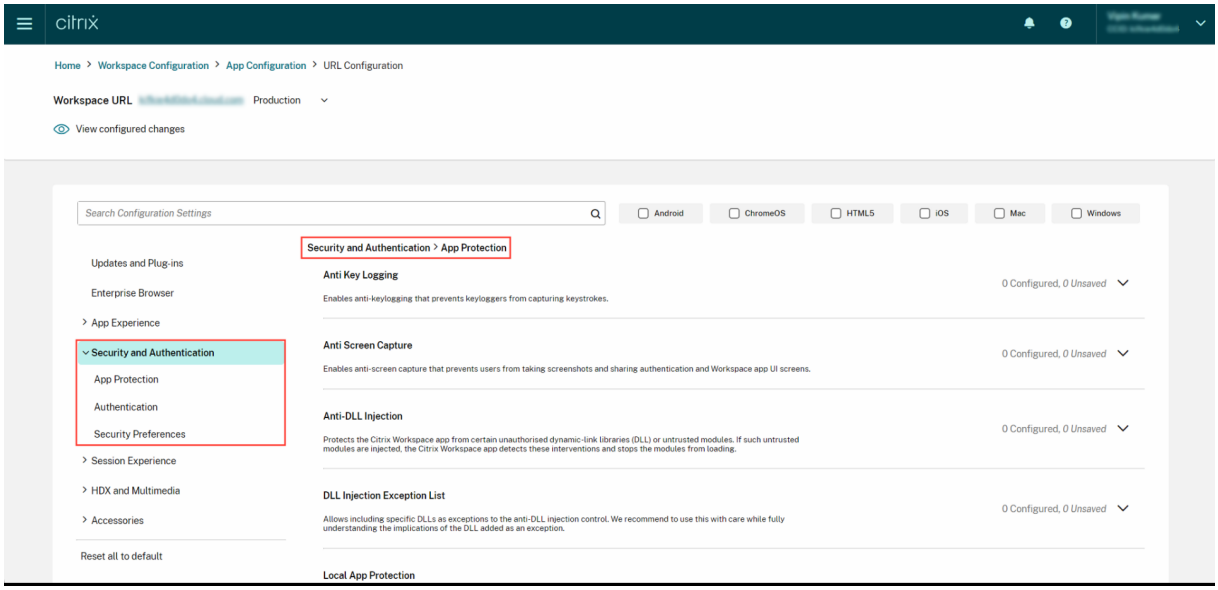


## Sep 28, 2023

### Simplified settings categorization for easy navigation

The Global App Configuration service UI has been enhanced to deliver a user-friendly categorization of settings. The settings have been categorized based on end-user workflows and topics, comprising seven primary folders and multiple subfolders. This clutter-free organization makes it easier for admins to navigate among 300+ settings.

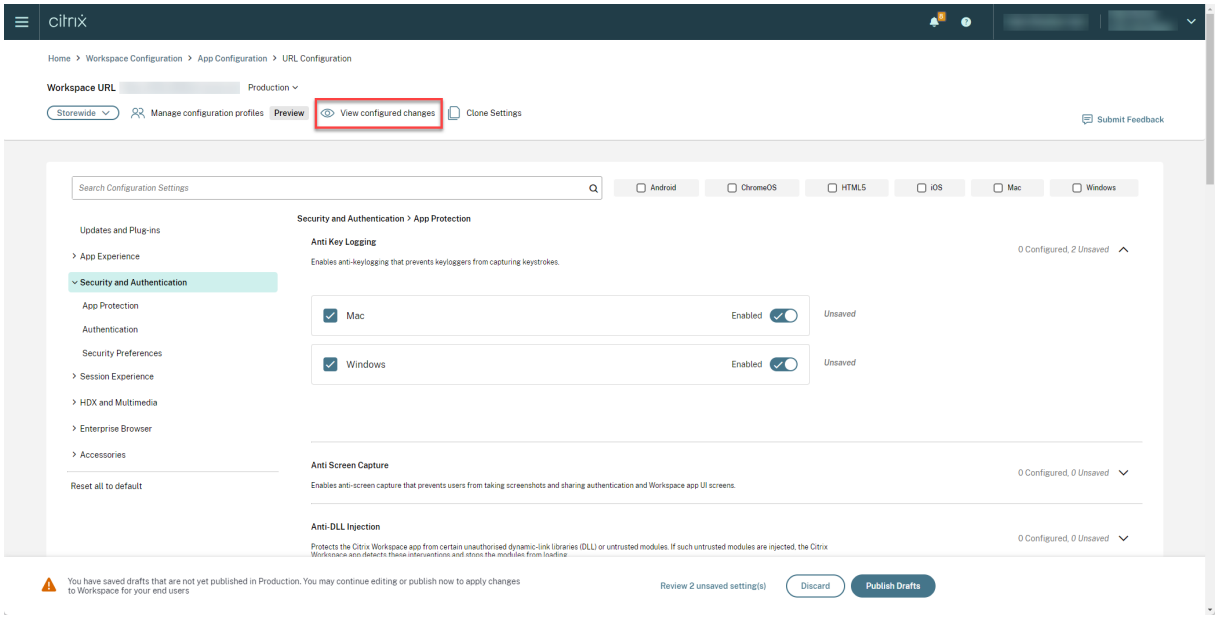



## Jul 28, 2023

### View summary of configured settings

Admins can now view a summary of the current configuration by clicking the **View configured settings** button. This eliminates the need to expand and review each setting separately. A consolidated list of all the configured settings allows admins to perform a comprehensive review of the current configuration and gauge the user impact.

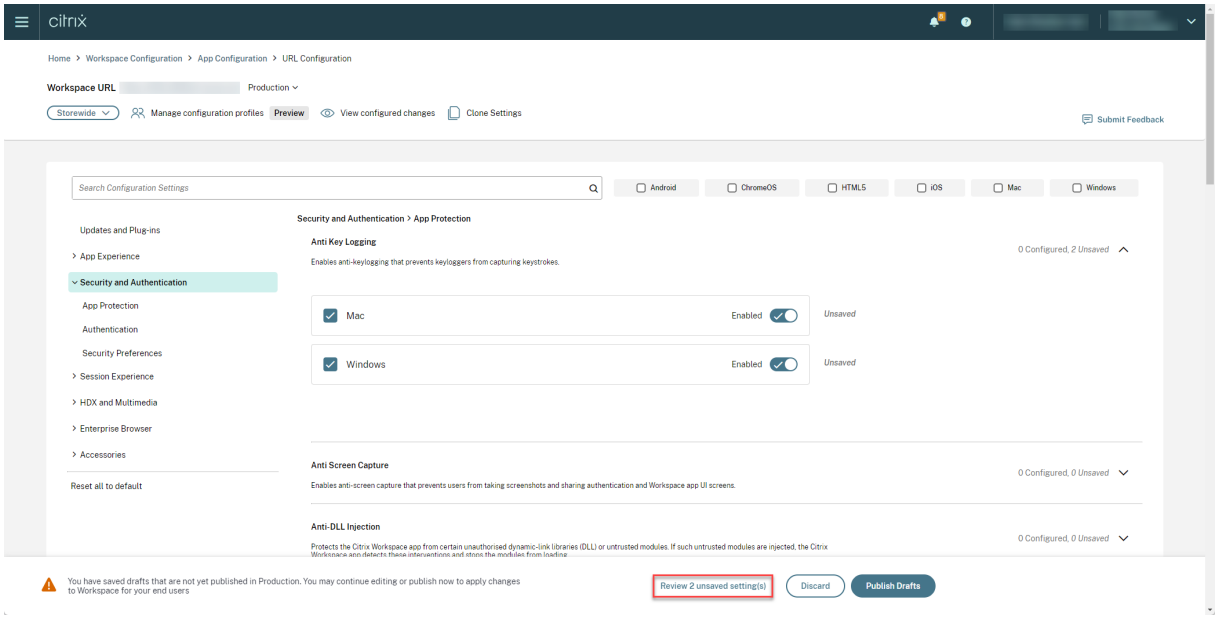
 




## Jun 07, 2023

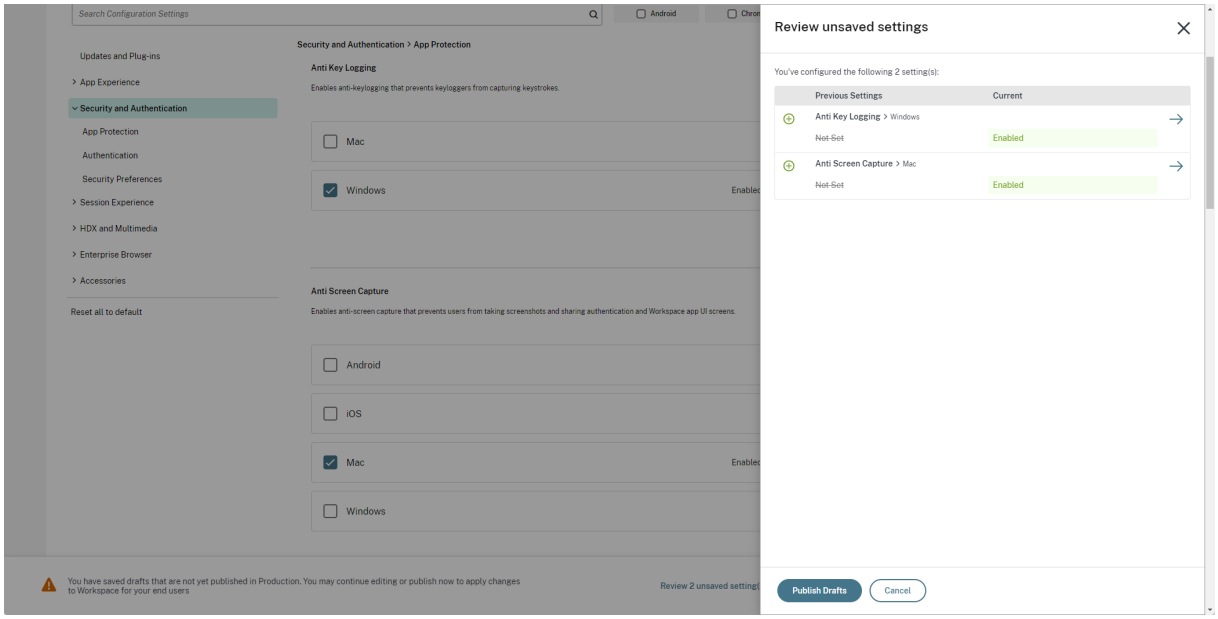
### Review unsaved changes

With this enhancement, admins can perform a final review of their unsaved changes before publishing the configuration. The number of unsaved settings is displayed on the UI and admins can access this list by clicking the **Review unsaved setting(s)** option. This enables admins to make informed changes and maintain data accuracy.




Admins can also navigate to an unsaved setting by clicking the arrow.

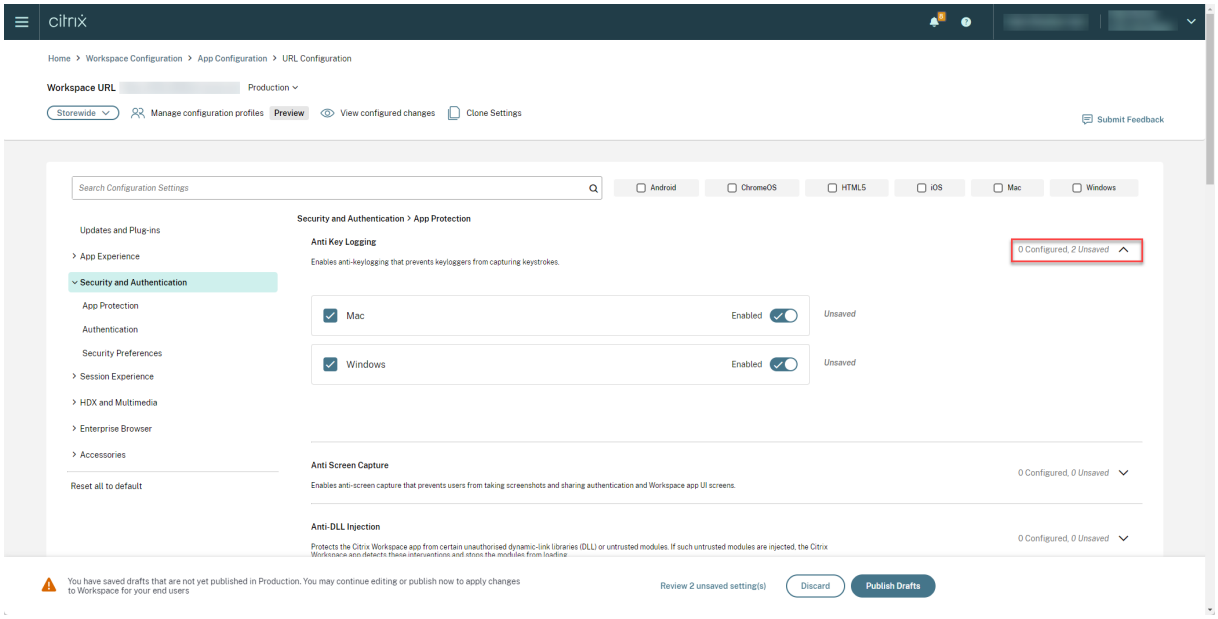
 




## Enhanced user interface

Admins can now view the status of each setting without expanding it.The following tags are now displayed to facilitate informed decision making at every step.

- **Configured**: Displays the number of platforms (client OS) for which the setting has already been configured.
- **Unsaved**: Displays the number of settings that are configured but not yet saved



## May 23, 2023

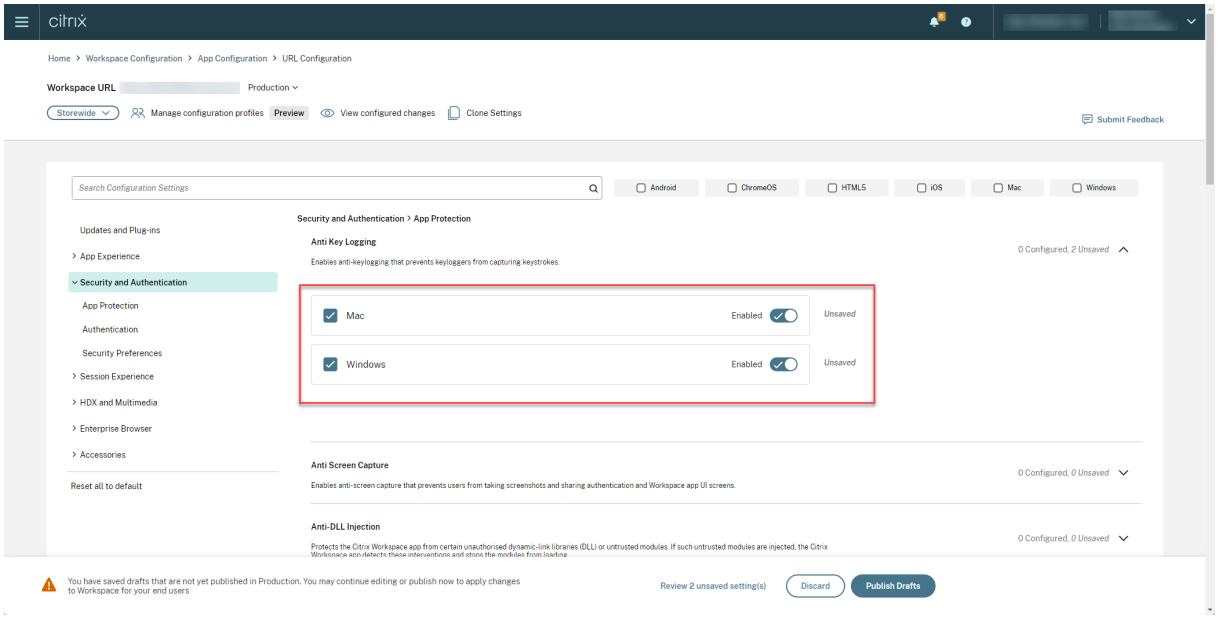
### Enhanced search capabilities

With this enhancement, 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 App Configuration page with ease. They can use the following search methods.

- **Search using setting description**
  Admins can also locate settings by entering keywords found within the setting's description. This allows for a more flexible search approach, utilizing relevant terms associated with the desired setting.
- **Search using API setting name**
  Admins have the option to 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 is relevant and applicable. This intelligent filtering ensures that users are presented with a concise and tailored list of options, eliminating unnecessary clutter and confusion.



# Configure settings for cloud stores

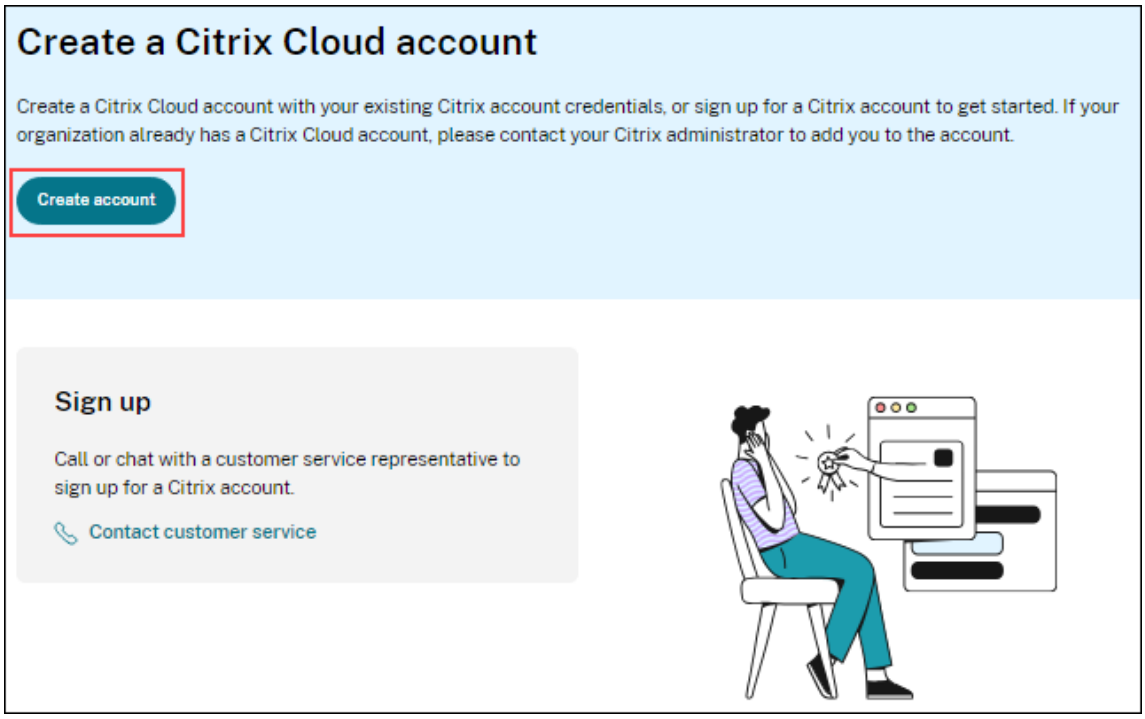
June 22, 2026

## Overview

You can configure Citrix Workspace™ app settings for cloud stores using the Global App Configuration service (GACS). It helps admins configure and manage Citrix Workspace app for end users on both managed and unmanaged devices. This service is supported on Windows, Mac, Android, iOS, HTML5, and ChromeOS platforms.

## Prerequisites

- The addresses <https://discovery.cem.cloud.us>, <https://gacs-discovery.cloud.com>, and <https://gacs-config.cloud.com> must be contactable. It's required for the functioning of email-based discovery and Global App Configuration service.
- 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.



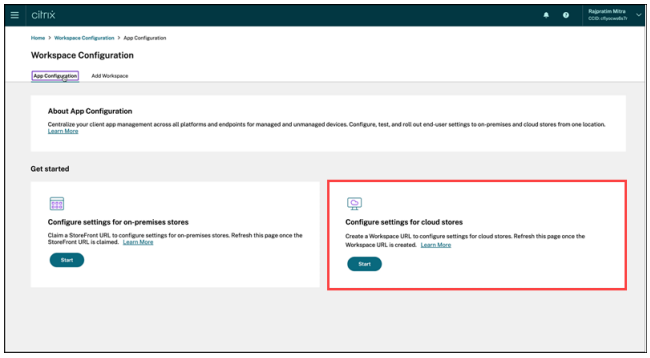

- Verify that you have a Citrix® StoreFront Cloud subscription.

## Get started with configuration

You can sign in to your Citrix Cloud™ account and configure settings from **StoreFront Cloud** > **App configuration**.
Before proceeding, verify if you have the following permissions.

- **store subscription:** The Citrix® StoreFront Cloud subscription is required to create a store URL. If you don't have a subscription, you can't add and configure cloud stores. You'll only be presented with an option to configure on-premises stores.
- **store URL:** If you have a Citrix® StoreFront Cloud subscription but haven't added your URL yet, you are presented with the following screen.

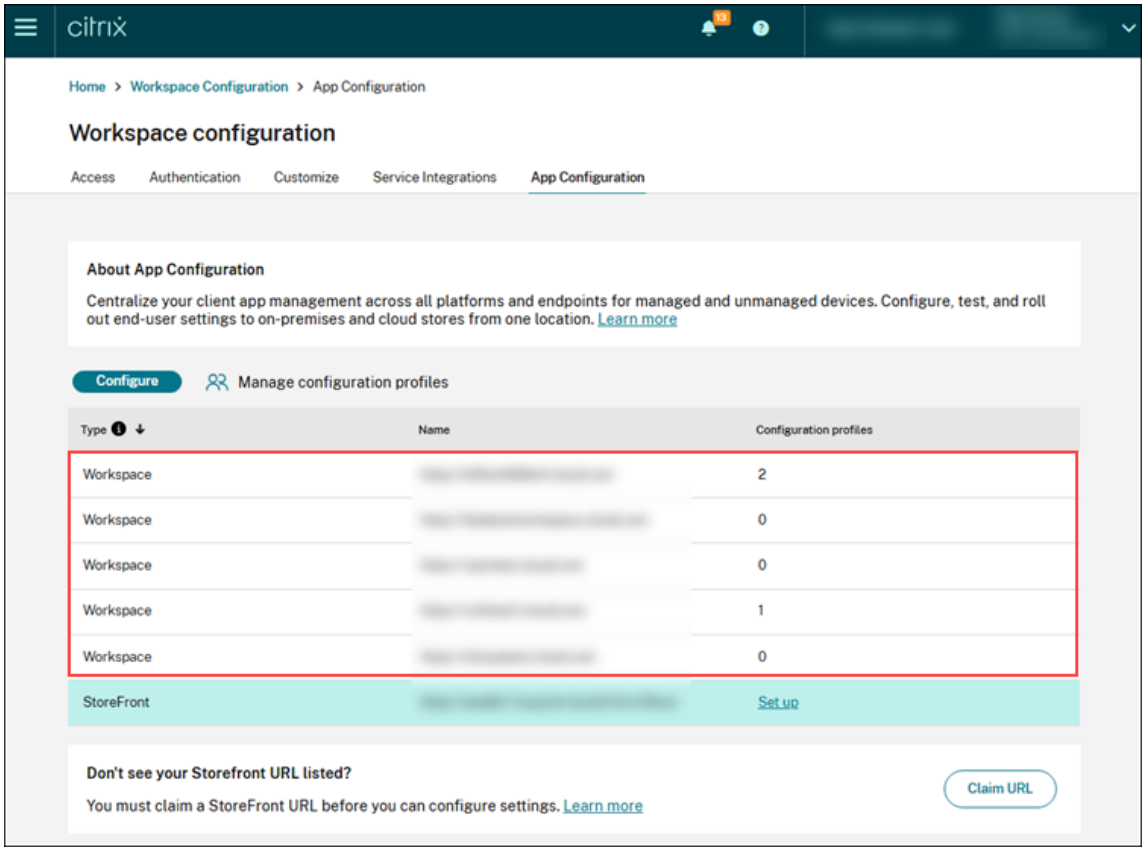



## Configure settings

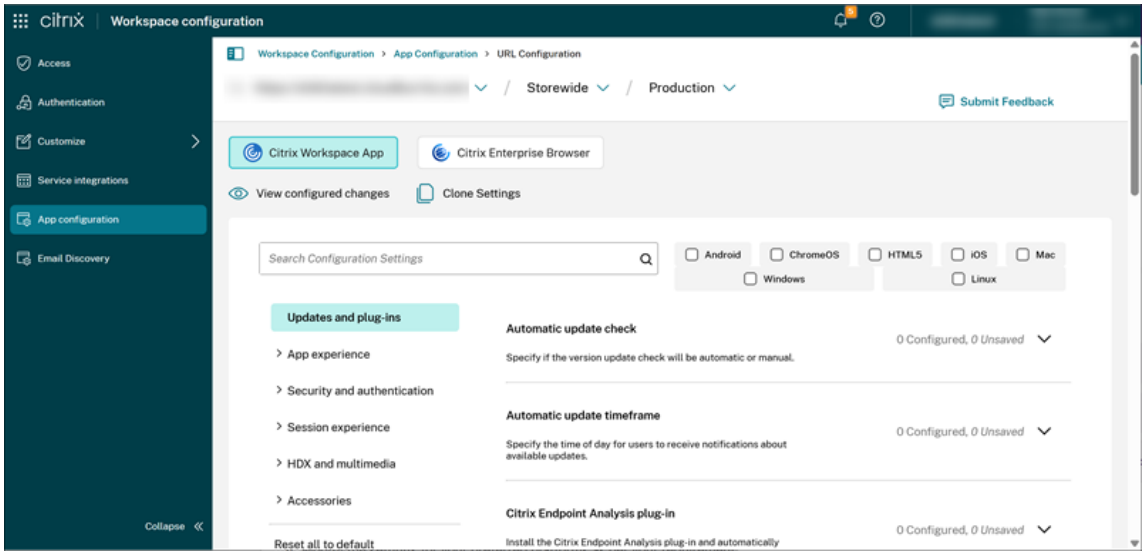
You can configure settings for Citrix Workspace app from the Citrix Cloud portal. If multiple stores have been configured for your organization, you can configure each of the stores separately.

1. Sign in to Citrix Cloud.
2. Navigate to **StoreFront Cloud** > **App configuration**.
3. From the list of configured store URLs, select the store for which you want to map settings and then click **Configure**.




4. Modify the settings for your preferred platforms as per your requirement.




5. Click **Publish Drafts** to save the settings.

> **Note:**
>
> It might take a few hours for the settings to be updated to the Citrix Workspace app clients. For

> more information, see Frequency of fetching updated settings.

### Manage settings for user group using configuration profiles

This section explains how administrators can use the configuration profile feature in the Global App Configuration service (GACS) to configure settings for user groups who use cloud stores of Citrix Workspace app.

To get started with this feature, administrators need to verify that their Citrix Workspace app version is compatible, as shown in the following table:

| Citrix Workspace app platform | Minimum supported version |
|---|---|
| Windows | 2405 |
| Mac | 2405.11 |

#### Configuration

For instructions on leveraging configuration profile to assign settings to a user group, see Manage settings for user group using configuration profile.

## Configure settings for on-premises stores

June 22, 2026

### Overview

You can configure the Citrix Workspace™ app settings for on-premises stores using the Global App Configuration service (GACS). It helps you configure and manage Citrix Workspace app for end users on both managed and unmanaged devices. The Global App Configuration service is supported on Windows, Mac, Android, iOS, HTML5, and ChromeOS platforms.

### Prerequisites

- The addresses <https://discovery.cem.cloud.us>, <https://gacs-discovery.cloud.com>, and <https://gacs-config.cloud.com> must be contactable. It'

s required for the functioning of the email-based discovery and Global App Configuration service.

- Verify that you have access to a Citrix Cloud account. If you don't already have an account, you can create one from https://onboarding.cloud.com/. For more information, refer to Sign up for Citrix Cloud.
- In an on-premises environment, you must claim a URL before you can configure settings. For more information, see Claim a URL.

### Get started with configuration

To configure settings for an on-premises store, sign in to your Citrix Cloud account and navigate to **StoreFront Cloud** > **App configuration**. If you have claimed ownership for your StoreFront URL, see the Configure settings section for more information.

If you haven't claimed your StoreFront™ URL yet, you can claim it. For that, click **Claim StoreFront URL** under the **App configuration** section to claim your URL. For more information, see the Claim a URL for on-premises stores section.

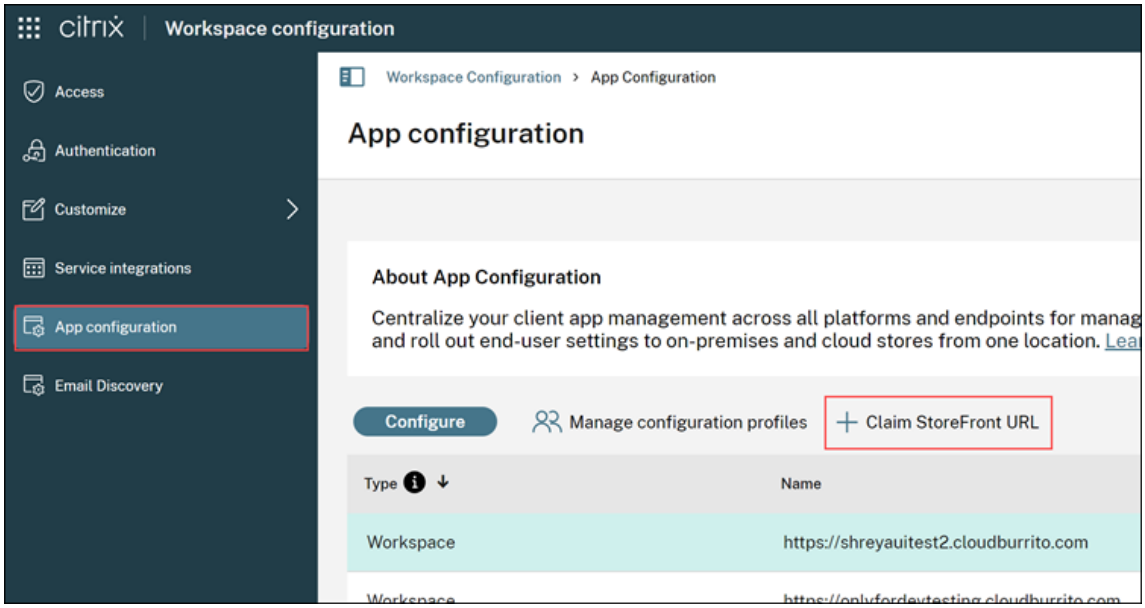
### Claim a URL for on-premises stores

It's mandatory to establish a claim to your URL before you start configuring the settings for it.

To claim a URL:

1. Sign in to Citrix Cloud.
2. Navigate to **StoreFront Cloud** > **App configuration**.
3. Click **Claim StoreFront URL**.

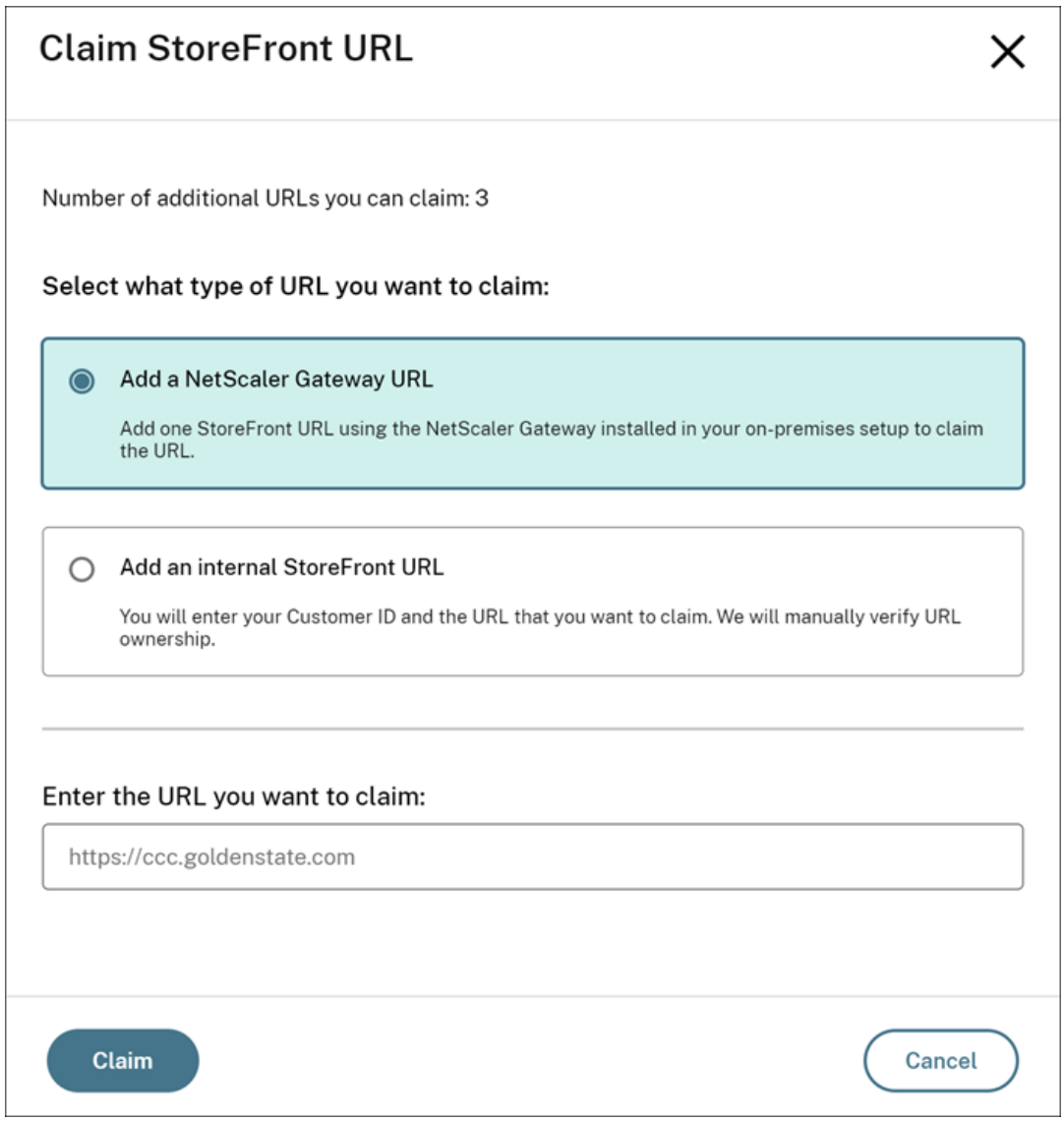



4. Select either **Add a NetScaler® Gateway URL** or **Add an internal StoreFront URL** based on your organization setup.

    - If you have a NetScaler Gateway installed in your on-premises setup, you can verify your URL using the following steps:

        a. Select **Add a NetScaler Gateway URL**.




b. Enter the URL in the given text field.

c. Click **Claim**.

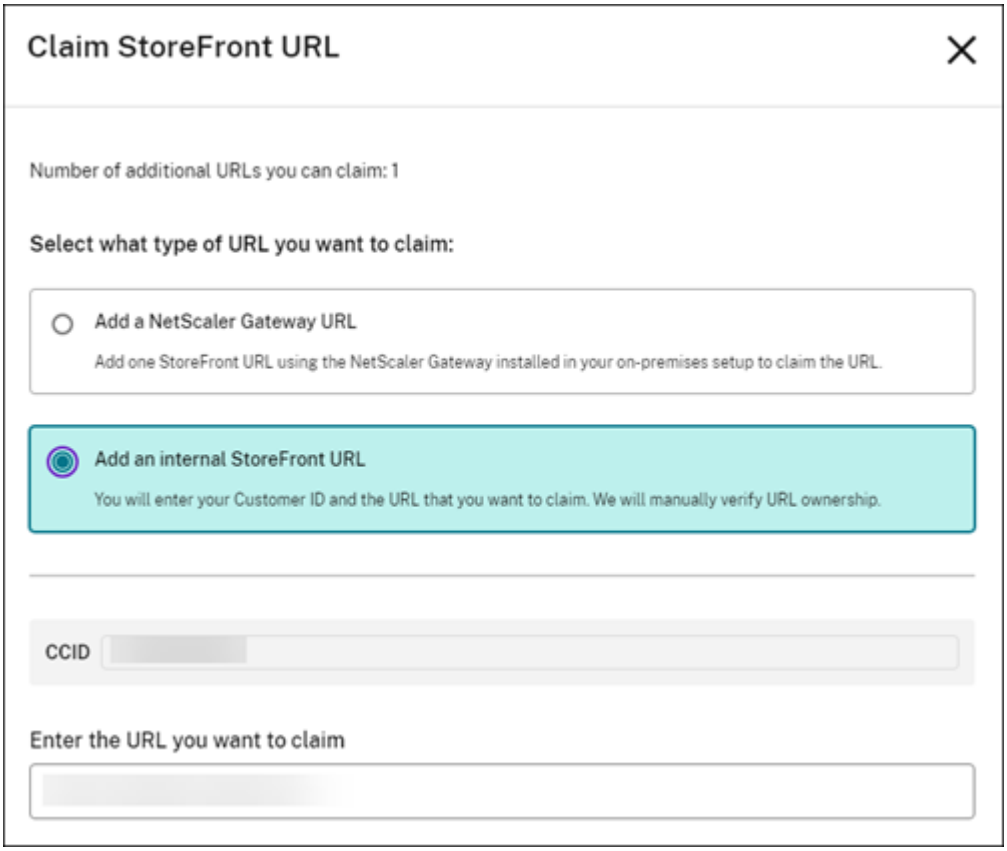
The URL is added, and it is in the 'Verification not started' state.

- If you want to claim a URL that is not NetScaler-based, do the following:

  a. Select **Add an internal StoreFront URL**.

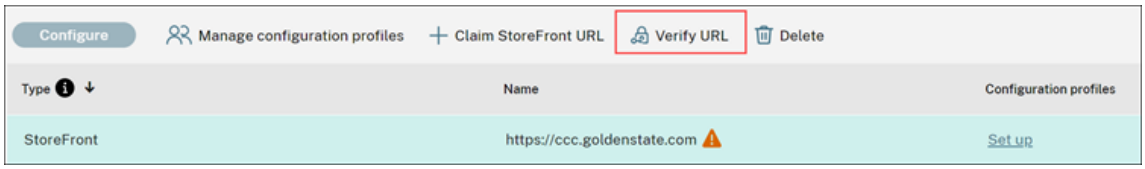
  b. Enter your Customer ID (CCID) and the URL you want to claim.



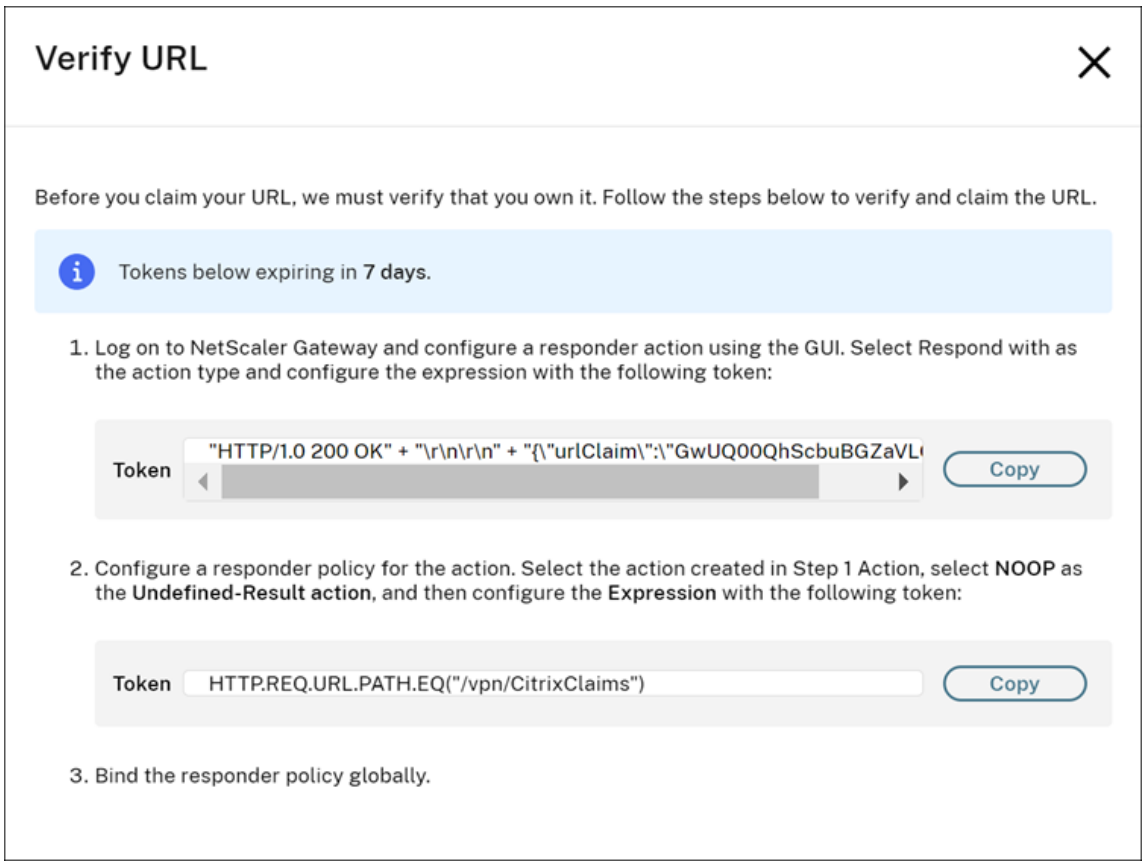

c. Click **Claim**.

5. To verify the URL, select the URL and click **Verify URL**.




6. 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 **StoreFront Cloud** > **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.

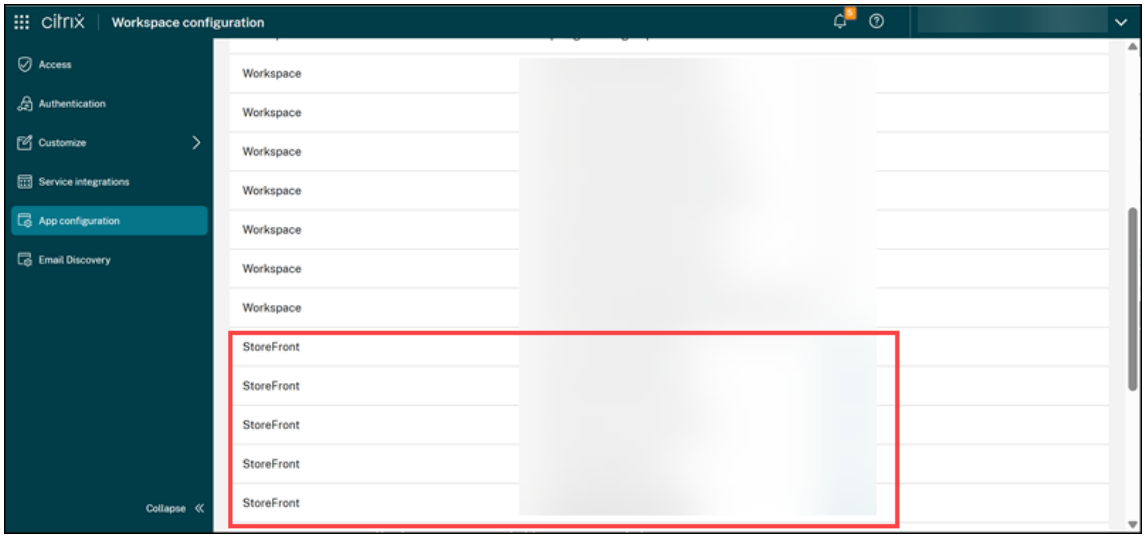
### Configure settings

You can configure settings for Citrix Workspace app, once you've claimed the URL. If multiple stores have been configured for your company, you can configure the settings for each of them separately.

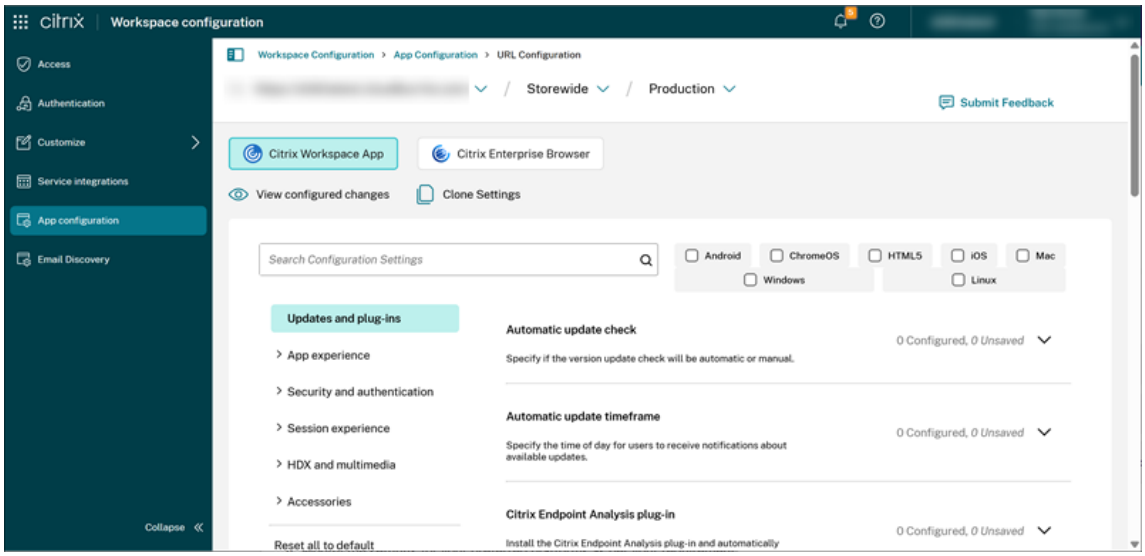
1. Go to the Citrix Cloud portal and sign in using your credentials.
2. Navigate to **StoreFront Cloud** > **App configuration**.

3. From the list of configured StoreFront URLs, select the one for which you want to map settings, and then click **Configure**.




4. Modify the settings for your preferred platforms as per your requirement.




5. Click **Publish Drafts** to save the settings.

> **Note:**
>
> It might take a few hours for the settings to be updated to the Citrix Workspace app clients. For more information, see Frequency of fetching updated settings.

### Manage settings for user group using configuration profiles

This section explains how administrators can use the configuration profile feature in the Global App Configuration service (GACS) to configure settings for user groups who use on-premise stores of Citrix

Workspace app.

### Prerequisites

To get started with this feature, 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** Verify your Citrix Workspace app version is equal to or higher than the versions specified in the following table.

| Citrix Workspace app platform | Minimum supported version |
|---|---|
| Windows | 2405 |
| Mac | 2405.11 |

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

**Configure 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 GACS. As a result, GACS can collect information about the AD group they belong to for managing configuration profiles.

The process involves the following steps:

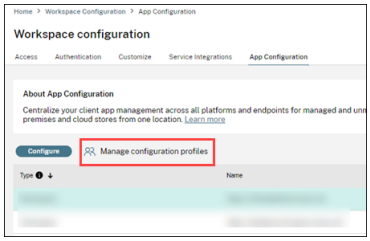
 

1. Generate registration tool.
2. Download and run the registration tool.
3. Validate the registration tool.

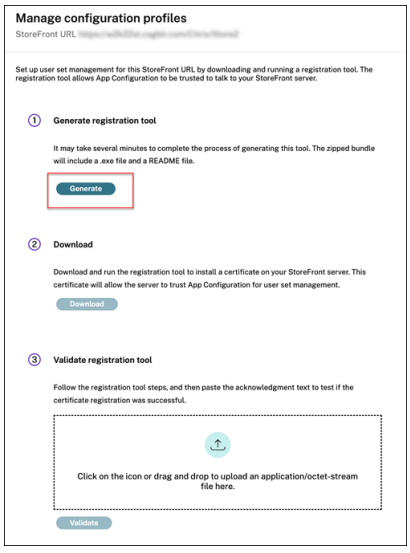
**Generate registration tool** The registration tool is an executable file that needs to be run on the StoreFront server hosted within the organization. This registers GACS as a trusted service to access AD group information.

To generate the registration tool, do the following:

1. Navigate to **StoreFront Cloud** > **App configuration**.
2. Select your StoreFront URL, and click **Manage configuration profiles**.

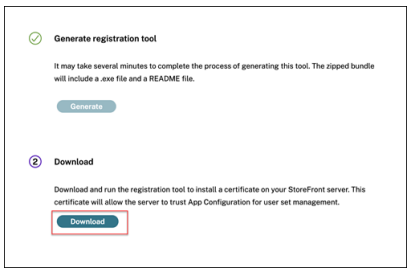



3. On the **Manage configuration profiles** screen, click **Generate** to generate the registration tool.




**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.

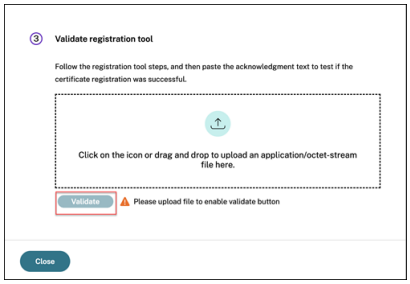
**Run the executable file**: Once the registration tool is downloaded, the administrator can then run the registration tool to install a certificate on the StoreFront server hosted within the organization. This certificate allows the server to trust GACS for the configuration profile management.

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 GACS to process incoming secondary tokens issued by the StoreFront server in order to provide authenticated, group-based settings to the client endpoint devices running Citrix Workspace app.
- **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.

1. Click the **Close** button, and you can see the **Manage configuration profiles** screen.

**Configuration** For instructions on leveraging configuration profile to assign settings to a user group, see Manage settings for user group using configuration profile.

## Email based discovery

June 22, 2026

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:

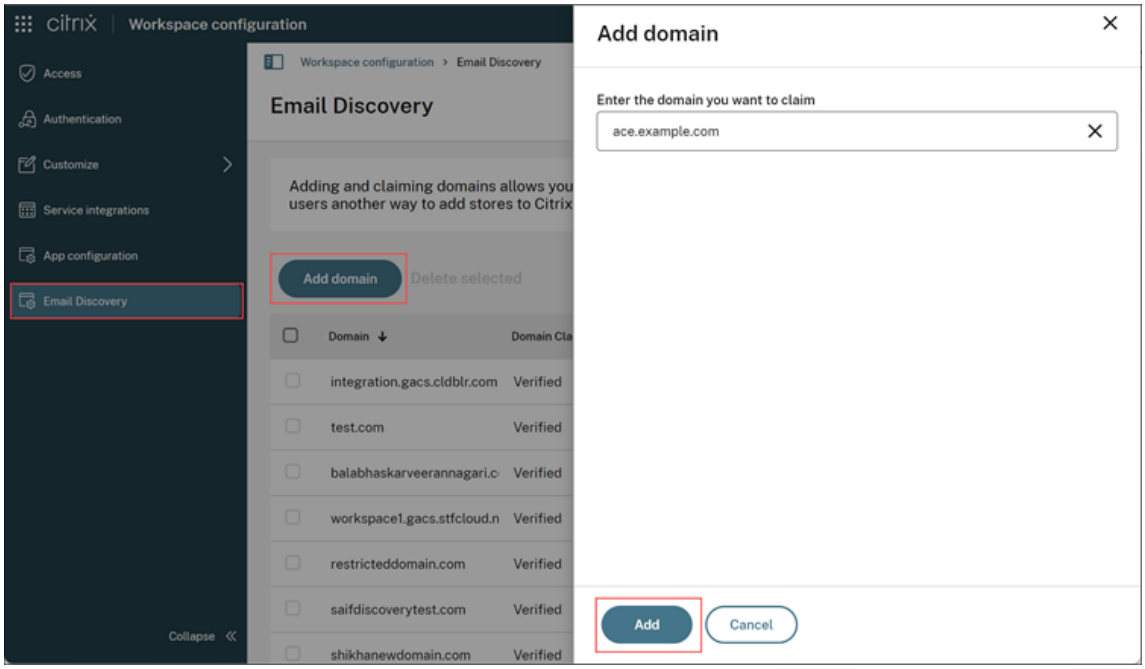
1. Claim a domain
2. Create a domain to URL mapping

#### Claim a domain

To claim a domain:

1. Sign in to Citrix Cloud.
2. Navigate to **StoreFront Cloud** > **Email Discovery**.
3. Click **Add Domain**.
4. Enter the domain that you want to claim (For example, `ace.example.com`).

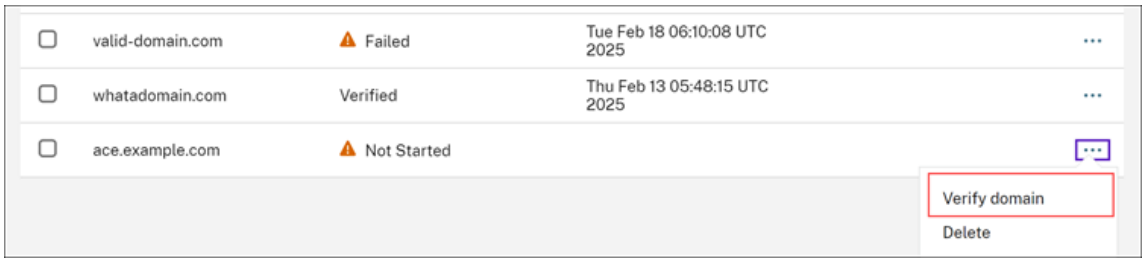



5. Click **Add**.

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

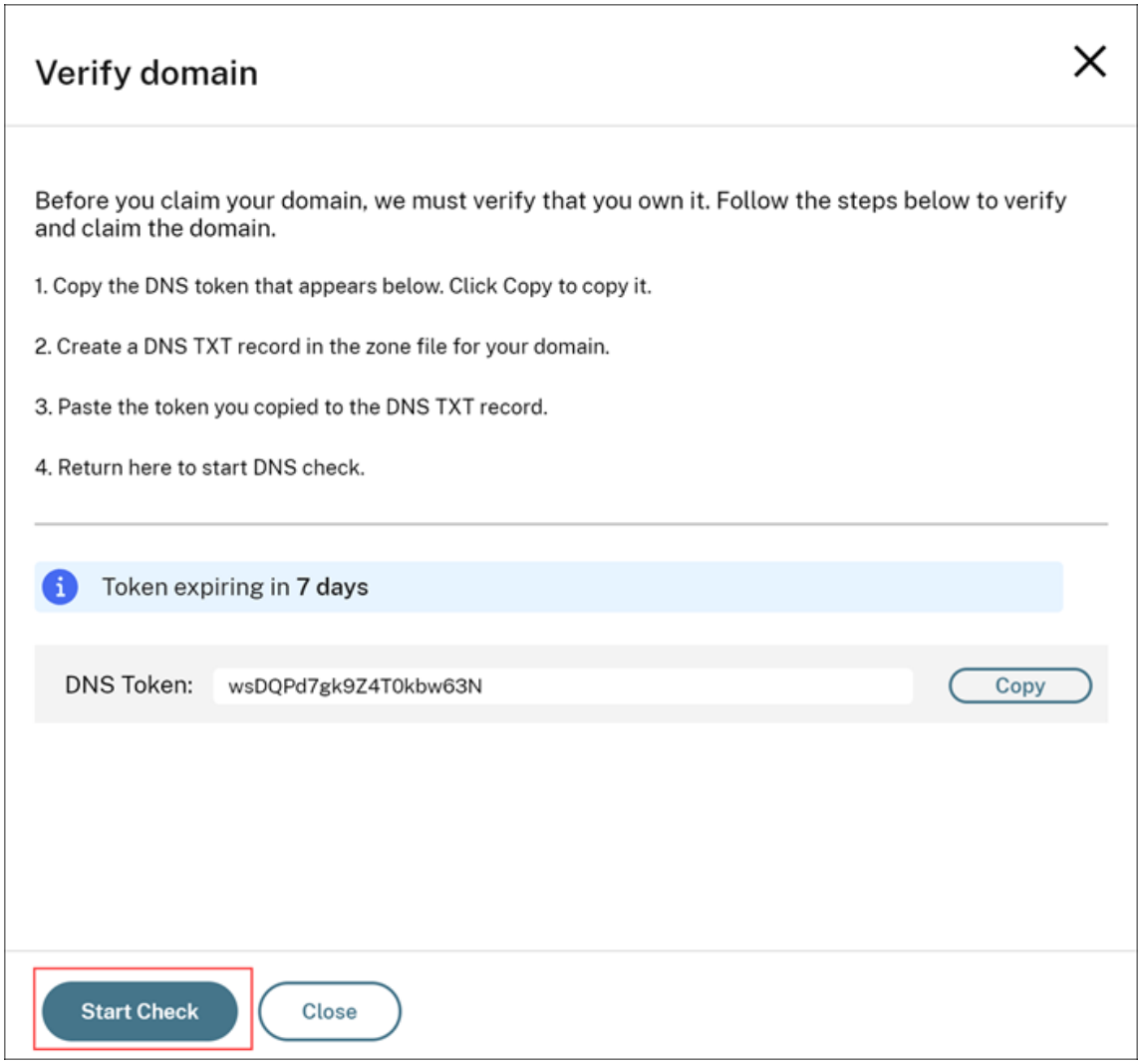
   The domain claim status is shown as **Not Started**. You need to verify the domain as shown in the following steps:

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**.

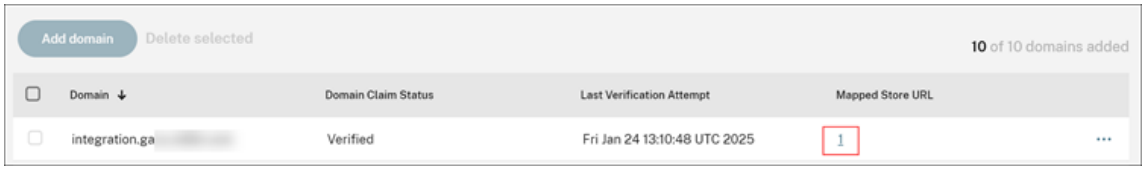
> **Note:**
>
> You can claim a maximum of 10 domains. If you want to claim more than 10 domains, contact Citrix Support and provide your Customer ID.

### Create a domain to URL mapping

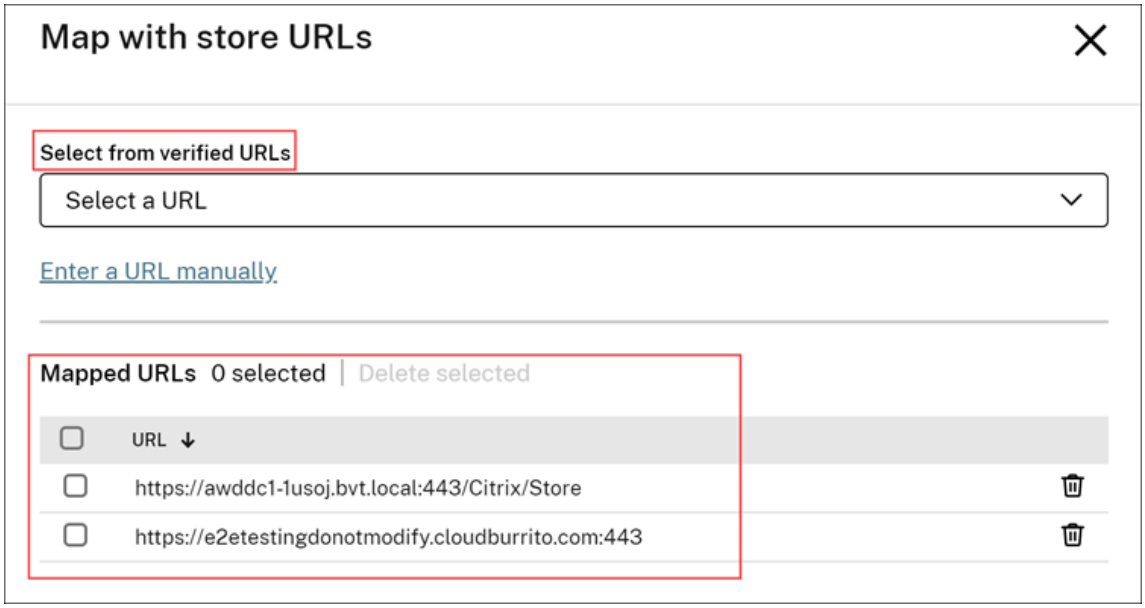
Once the domain is verified, you can map URLs as shown in the following steps:

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



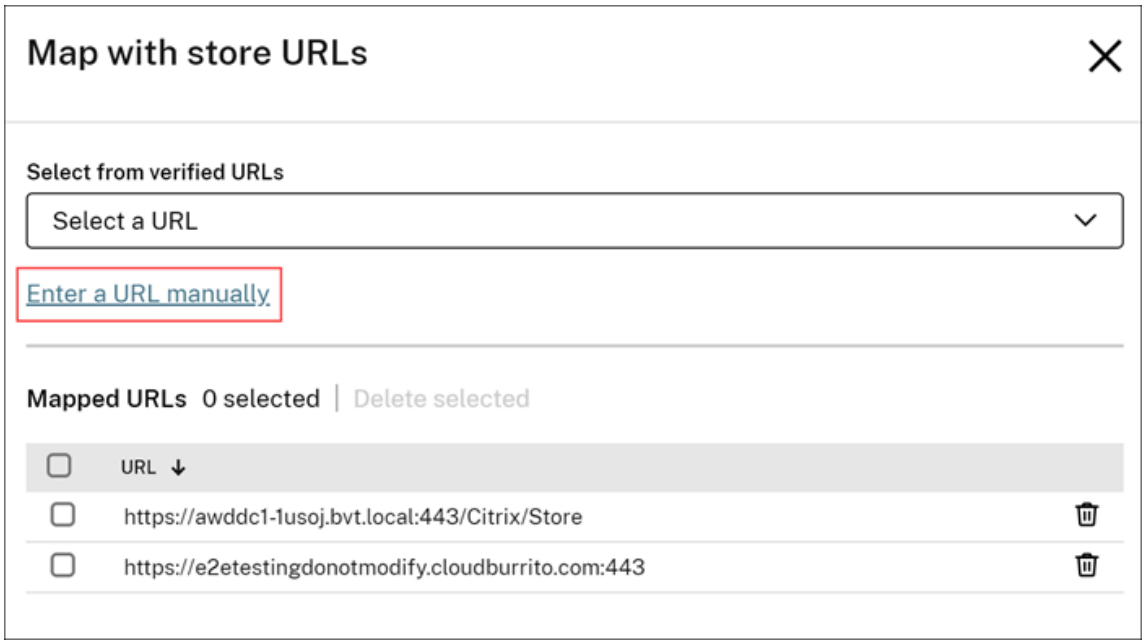

3. Select the claimed URLs from the dropdown menu.




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`.

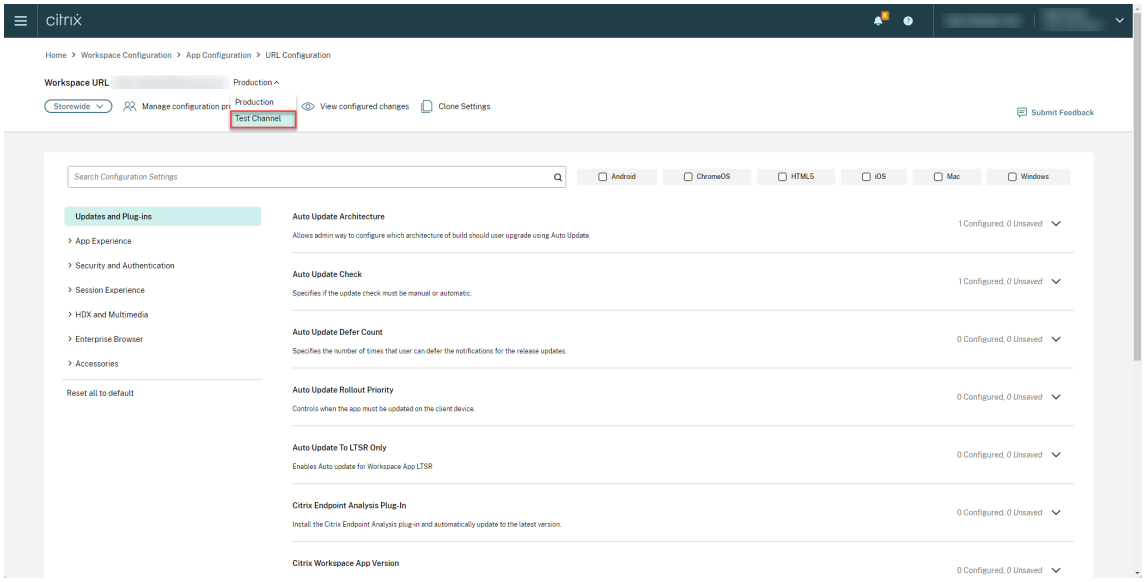
## Test channel configuration

June 22, 2026

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. On the main menu, navigate to **Client app management**.
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 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:**
>
> The Global App Configuration service 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 Global App Configuration service 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
```

Once 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.

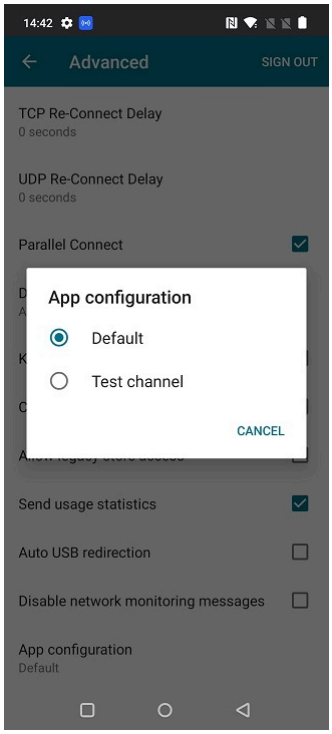
1. Sign in to the Citrix Workspace App.
2. Go to **Settings** > **Advanced** > **App configuration**.
3. Select the test channel.
4. You can now test the configuration defined by the admin.

### 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.
4. You can now test the configuration defined by the admin.




## Manage Citrix Workspace app versions

June 22, 2026

### Overview

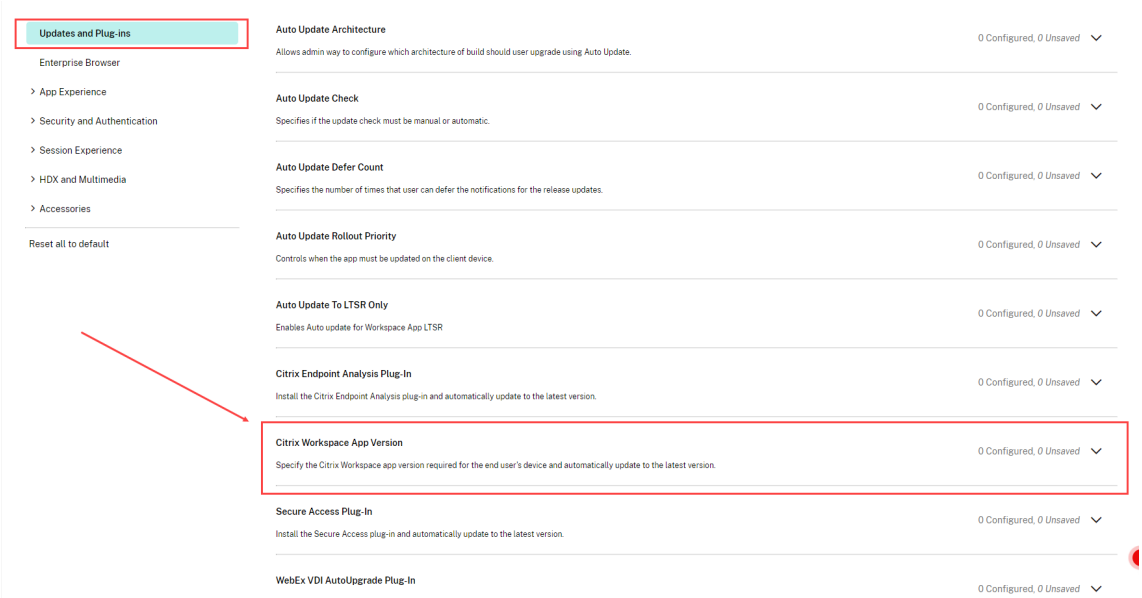
You can use the **Citrix Workspace App Version** setting to specify which Citrix Workspace app version must be used by your end users for optimal results. You can set up a rule that updates the app to the latest CR (Current Release) or LTSR(Long Term Service Release) version. You can also specify if the upgrade must occur automatically or if the end user can update the app manually.

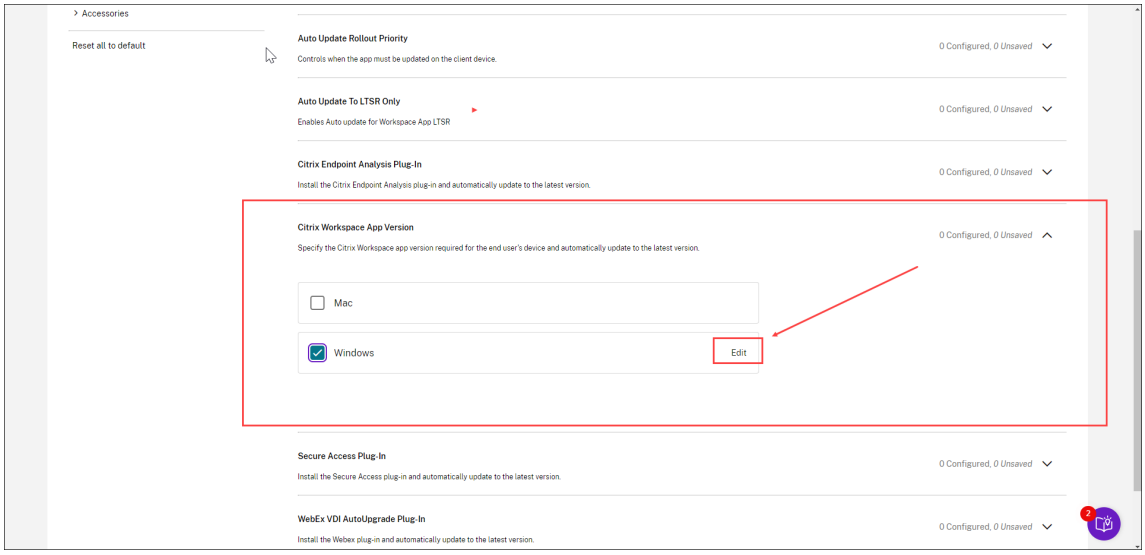
> **Note**
>
> This setting can be configured only for macOS and Windows OS.

To manage the app version settings, sign in to your Citrix Cloud™ console.

1. Navigate to **StoreFront Cloud > App Configuration**.
2. Go to the **Updates and Plug-ins** category.
3. Expand the **Citrix Workspace app Version** setting.




4. Select the Windows or Mac checkbox and then click **Edit**.




5. You can now customize the settings as explained in the Manage version settings section.
6. Save your settings.

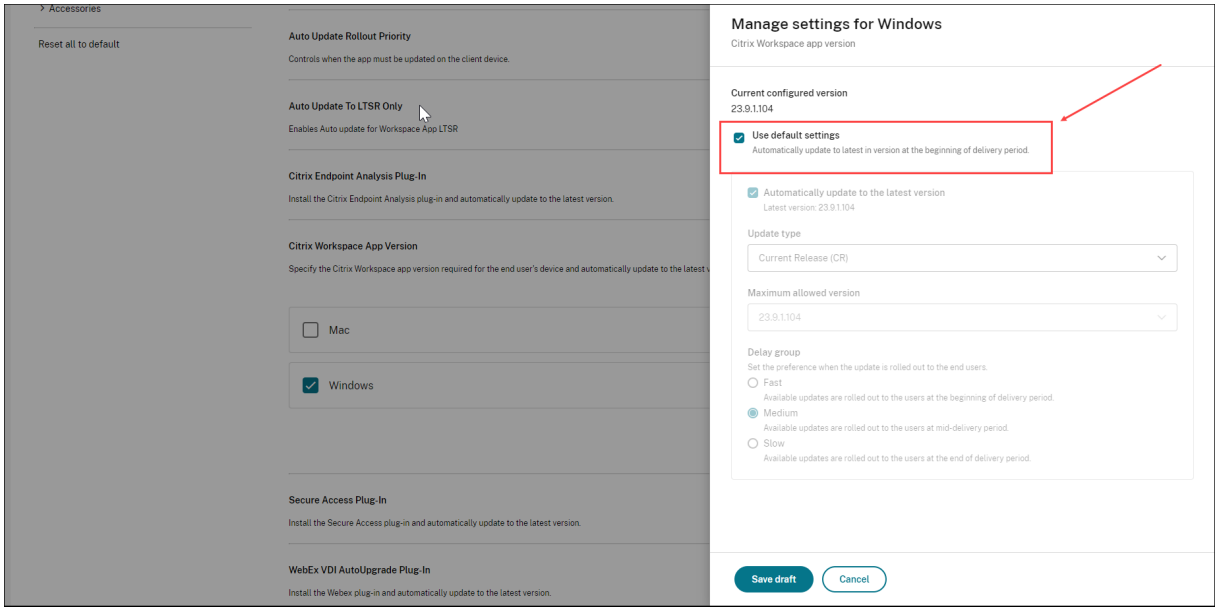
 

## Manage version settings

You can customize the Citrix Workspace app version settings to cover one of the following use cases.

### Upgrade your end users automatically to the latest CR version

If you select the **Use default settings** checkbox, your end users are updated to the latest CR version. The upgrade happens automatically at the beginning of the Delivery period, that is, as soon as a new CR version is rolled out. For more information on Delivery period, see Delay Group.



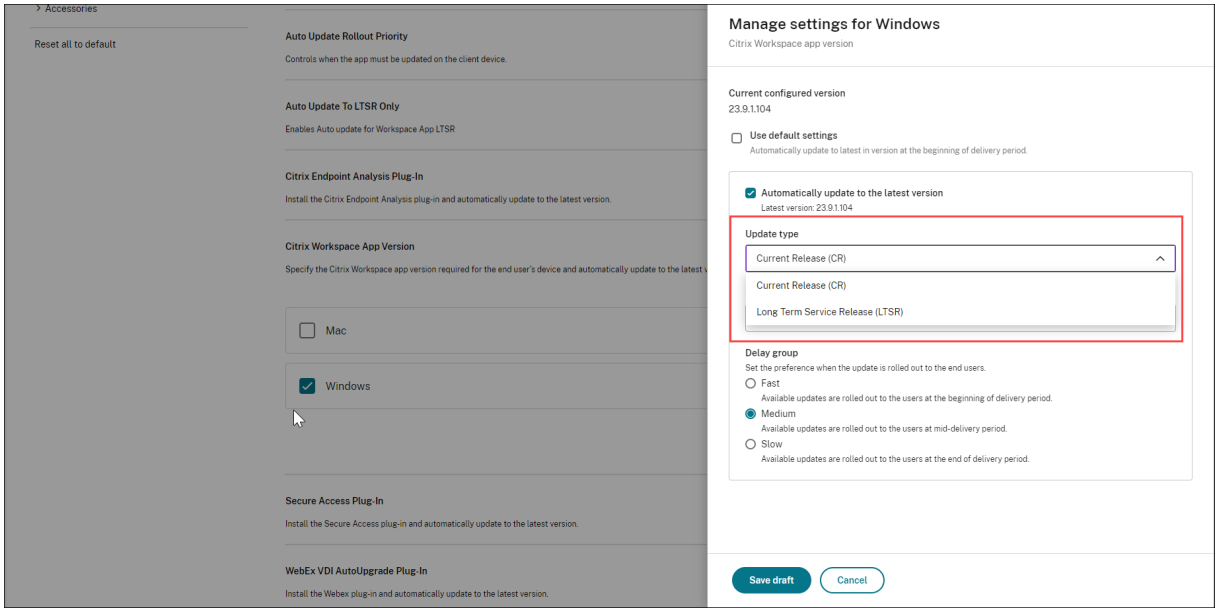

### Upgrade your end users automatically to the latest LTSR or CR version

The **Automatically update to the latest version** setting enables you to upgrade your end users to the latest version. However, you must select the delivery period for the upgrade under **Delay group** settings.

To use this option, you must first clear the **Use default settings** checkbox. Only then, you'll be able to select the **Automatically update to the latest version** setting. In the **Update Type** field, select LTSR or CR.

The upgrade occurs as per your Delay group settings. For example, if you have selected **Fast** under Delay group, the app is updated automatically as soon as a new version is rolled out. For more information on delivery period, see Delay group.



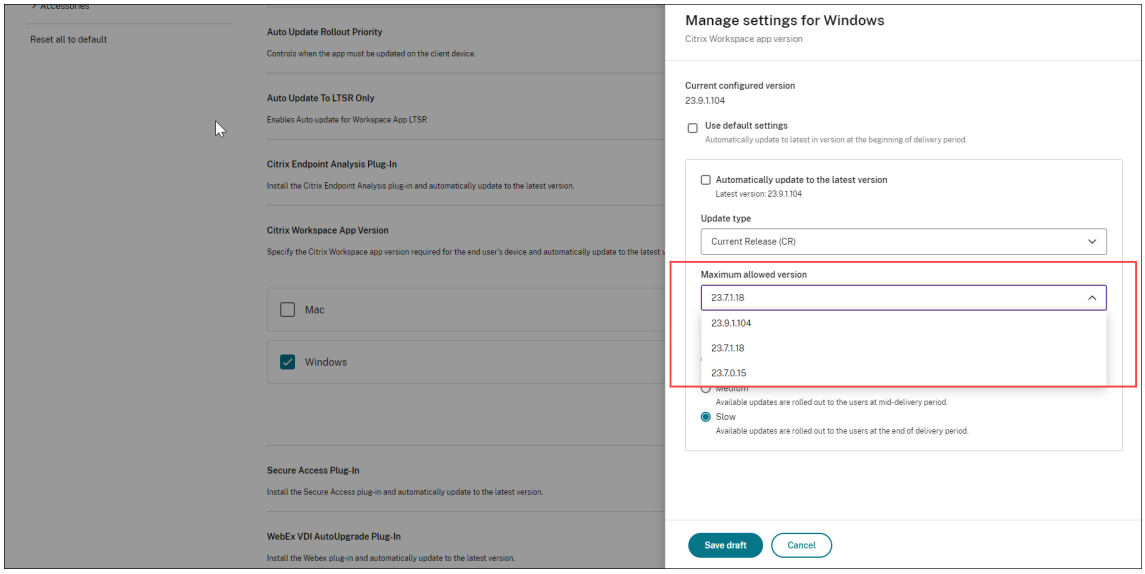

As the app is updated automatically to the latest version, the **Maximum allowed version** field is automatically disabled.

### Upgrade your end users to a specified CR or LTSR version

If you want to select a specific version that the end user must update to, proceed as follows.

1. Clear(disable) the **Use default settings** checkbox.
2. Clear(disable) the **Automatically update to the latest version** checkbox.
3. In the **Update type** field, select your preferred release type.
4. In the **Maximum allowed version**, select the version that you want to upgrade your end users to. You can select the appropriate version from a list of 3 previous versions.



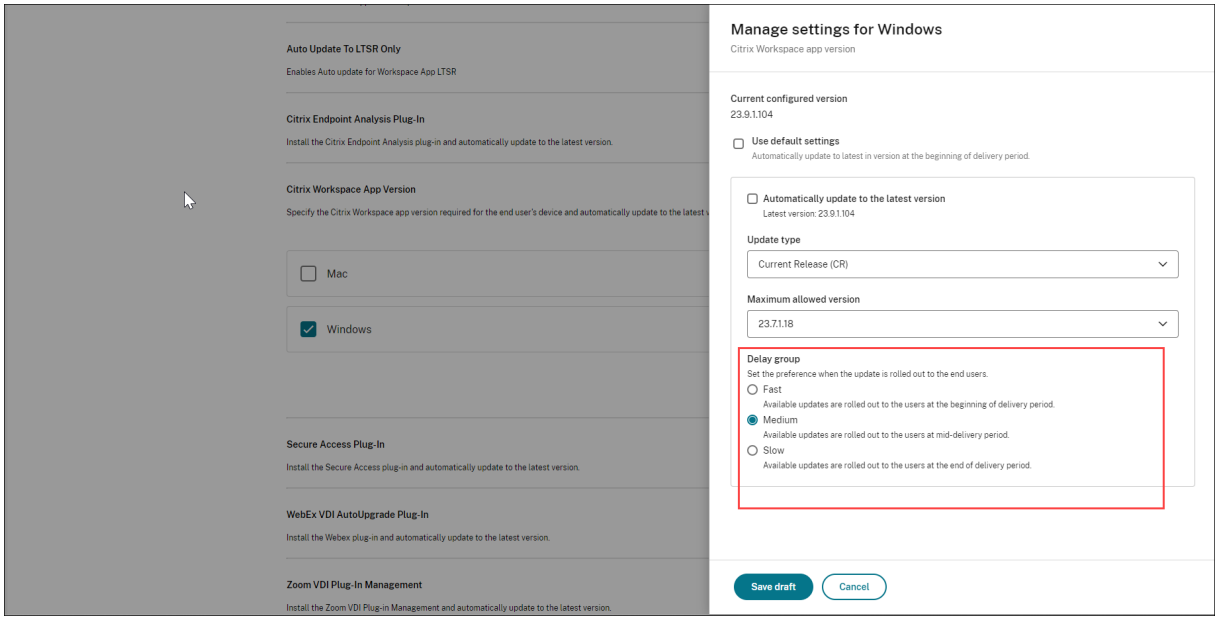

5. Under the Delay Group section, select the preferred delivery period. For more information on delivery period, see Delay Group.

## Delay Group

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

- **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.




## Automatic update timeframe

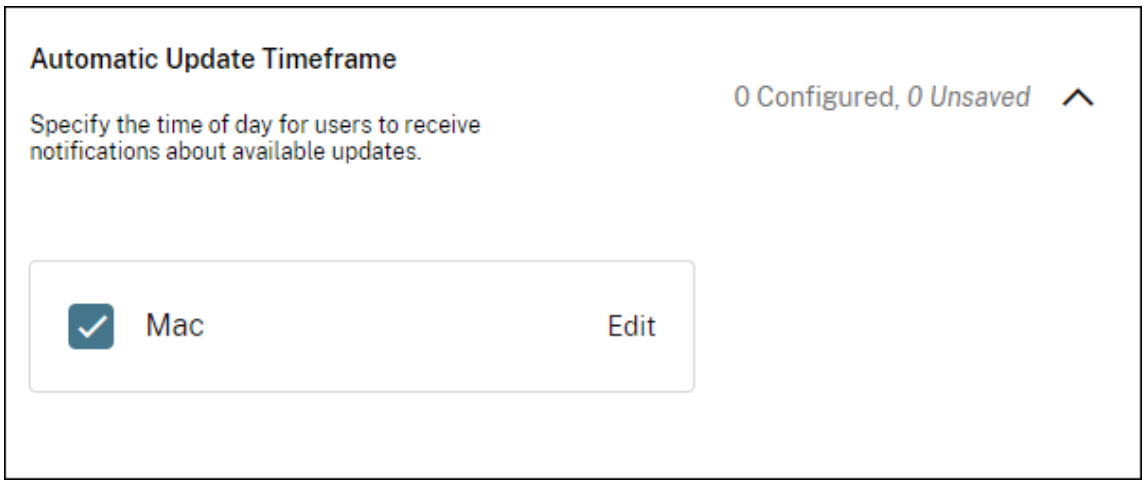
Administrators can now schedule automatic updates for Citrix® products at any preferred time on their Windows and Mac devices. During this specified time, software updates automatically or users receive notifications on available updates. This feature is applicable for all Citrix updates on Windows and Mac platforms. 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:

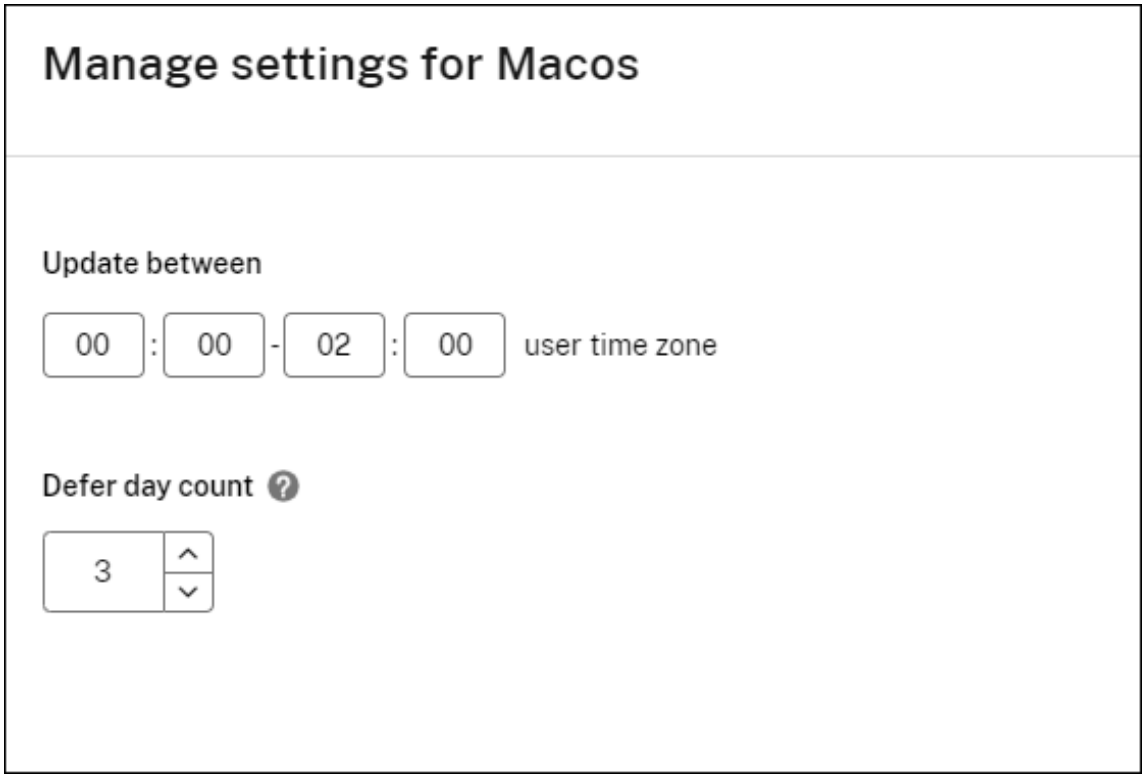
> **Note:**
>
> The feature is currently available only on the Windows and Mac platforms.

1. Navigate to **StoreFront Cloud** > **App Configuration** in Citrix Cloud.
2. Select the required store URL from the list.
3. Navigate to **Configure** > **Updates and Plug-ins**, and click the **Automatic update timeframe** setting.




4. Select 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 execute the automatic update.

> **Note:**
>
> The difference between start and end time should be at least 1 hour and should 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.

### Citrix Workspace app version

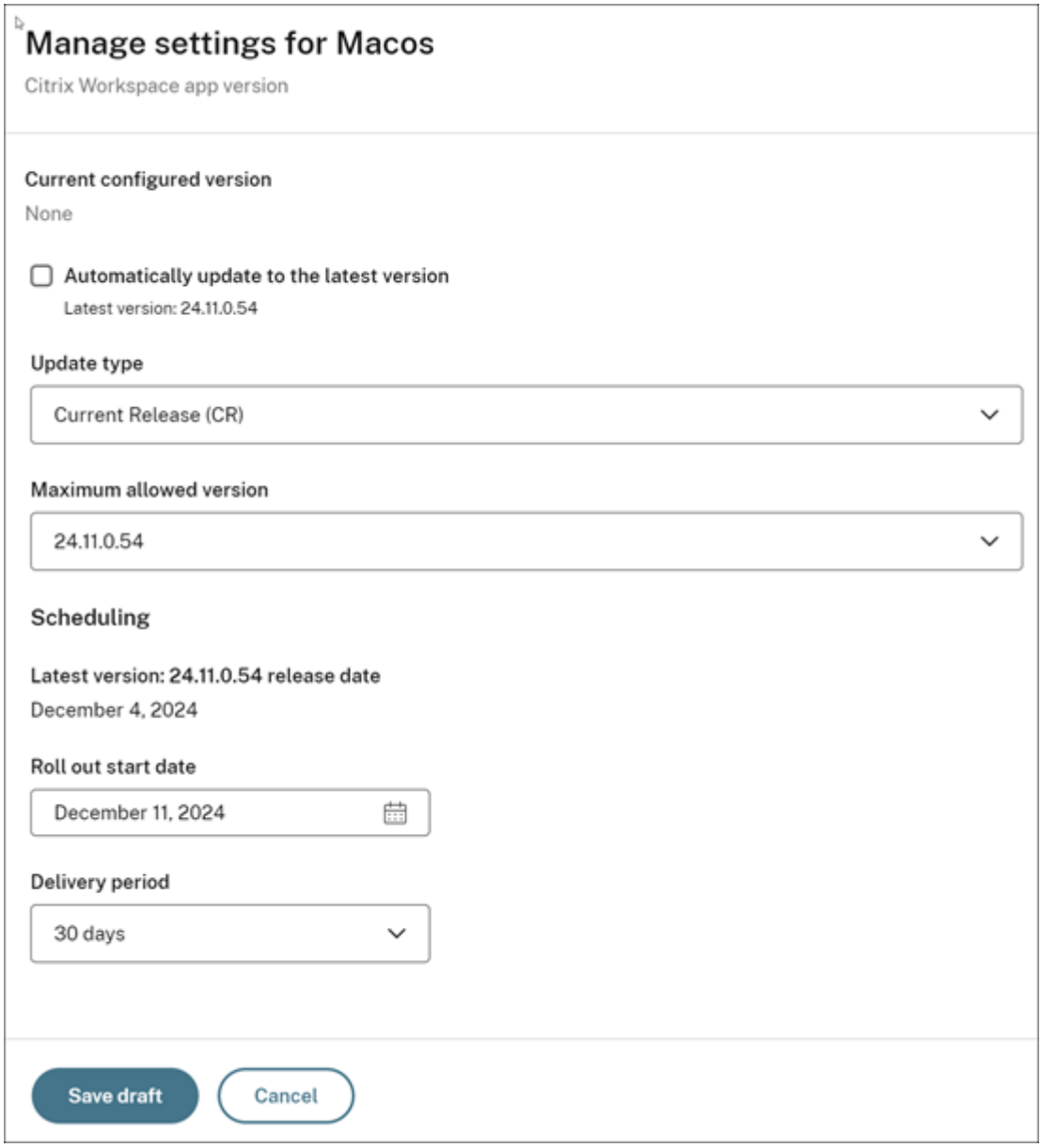
Administrators can schedule convenient date ranges during which an automatic update of Citrix Workspace app should roll out to their end users. This capability allows them to determine the rollout dates, minimizing disruption to end users and improving the user experience.

To enable this feature, do the following:

**Note:** The feature is currently available only for Citrix Workspace app on the Mac platform.

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




**Maximum allowed version**: Define the maximum software version 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. Once you set a date, the app doesn't get updated even if a newer version of the app is available.

**Delivery period**: Enter the number of days up to which the automatic update rolls out. The automatic update process will complete within the specified delivery period. The delivery period is an increment of 15.

> **Note:**
>
> Automatic updates occurs only after user sign in to Citrix Workspace app.

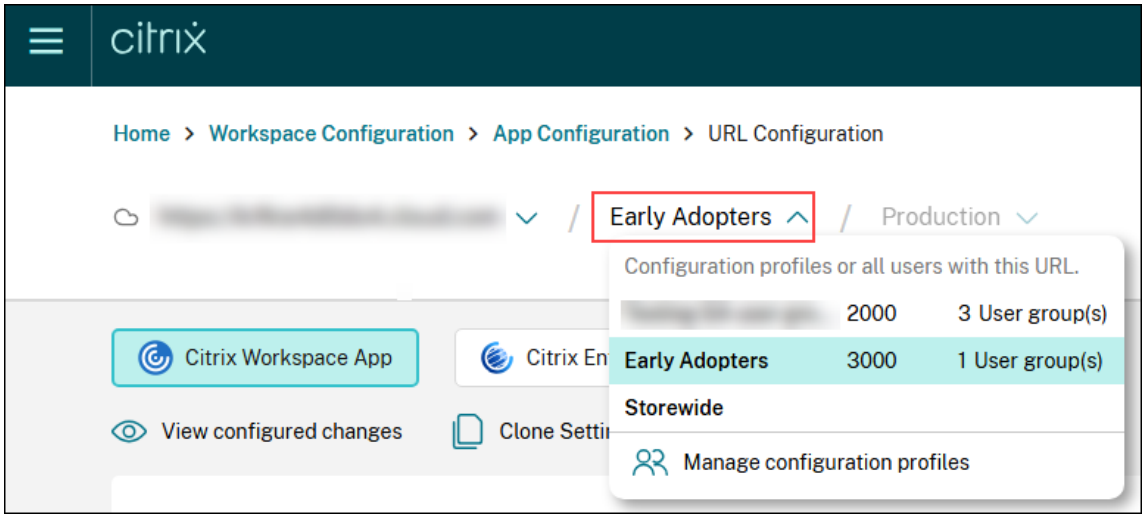
### Automatic update management settings supports configuration profiles

The automatic update management settings such as **Automatic update timeframe** and **Citrix Workspace app version** are applicable for different user groups through configuration profiles.

To enable this feature, do the following:

> **Note:**
>
> The feature is currently available only on the Mac platform.

1. Navigate to **StoreFront Cloud** > **App Configuration** in Citrix Cloud.
2. Select the required store URL from the list.
3. Navigate to **Configure**.
4. Select a configuration profile from the list.




5. Configure the settings **Automatic update timeframe** or **Citrix Workspace app version** as mentioned in Automatic update timeframe and Citrix Workspace app version.

## Manage plug-ins using Global App Configuration service

June 22, 2026

## Overview

With Global App Configuration service, you can configure installation and update settings for plug-ins from a centralized platform. These plug-ins must be built either by Citrix or its partners. The Global App Configuration service UI provides admins a centralized platform to distribute plug-ins across managed and personal devices.

> **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

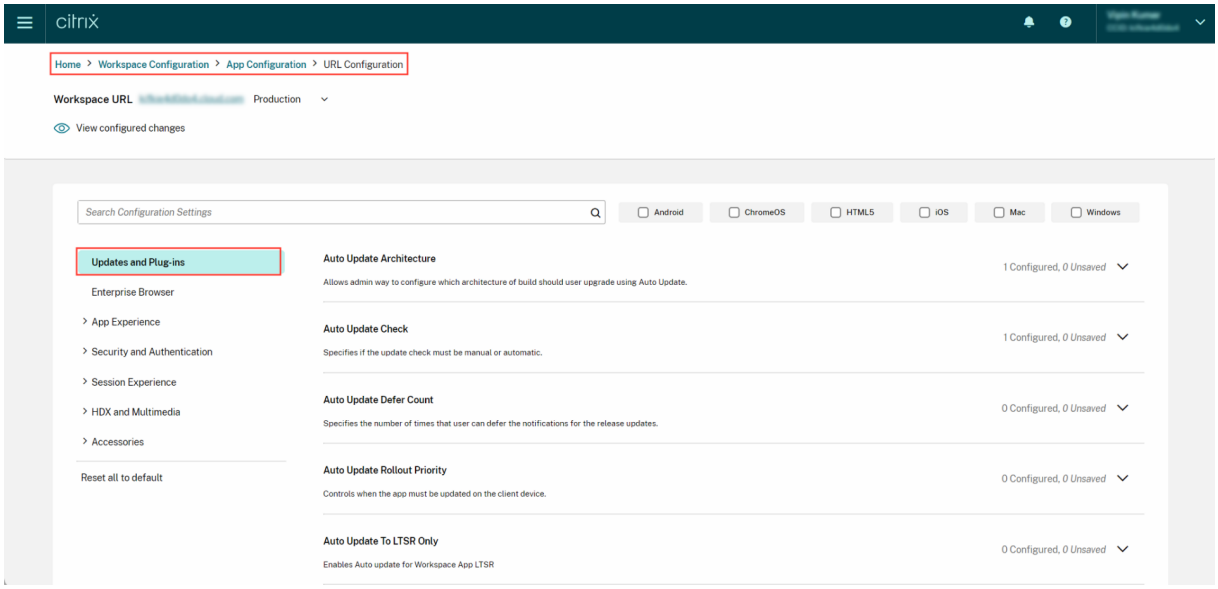
If your store is GACS configured and end users have already added it to their Citrix Workspace app, any change in the plug-in setting is reflected as per the duration specified here. This means that after you publish your changes, it might take a few hours for the settings to be updated on the client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

After the configuration has been fetched on the client side, the Citrix Auto-Update service installs the plug-in as per your **Delay Group** 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.

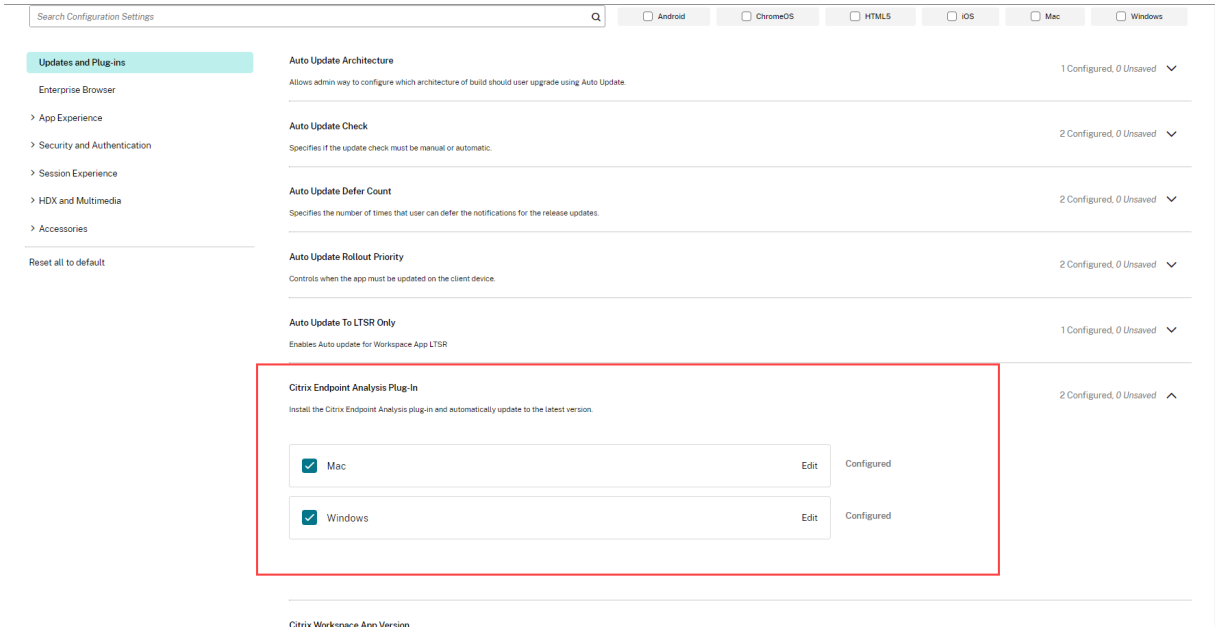
Supported plug-ins can be found under the **Updates and plug-ins** section on the GACS UI.




## 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.

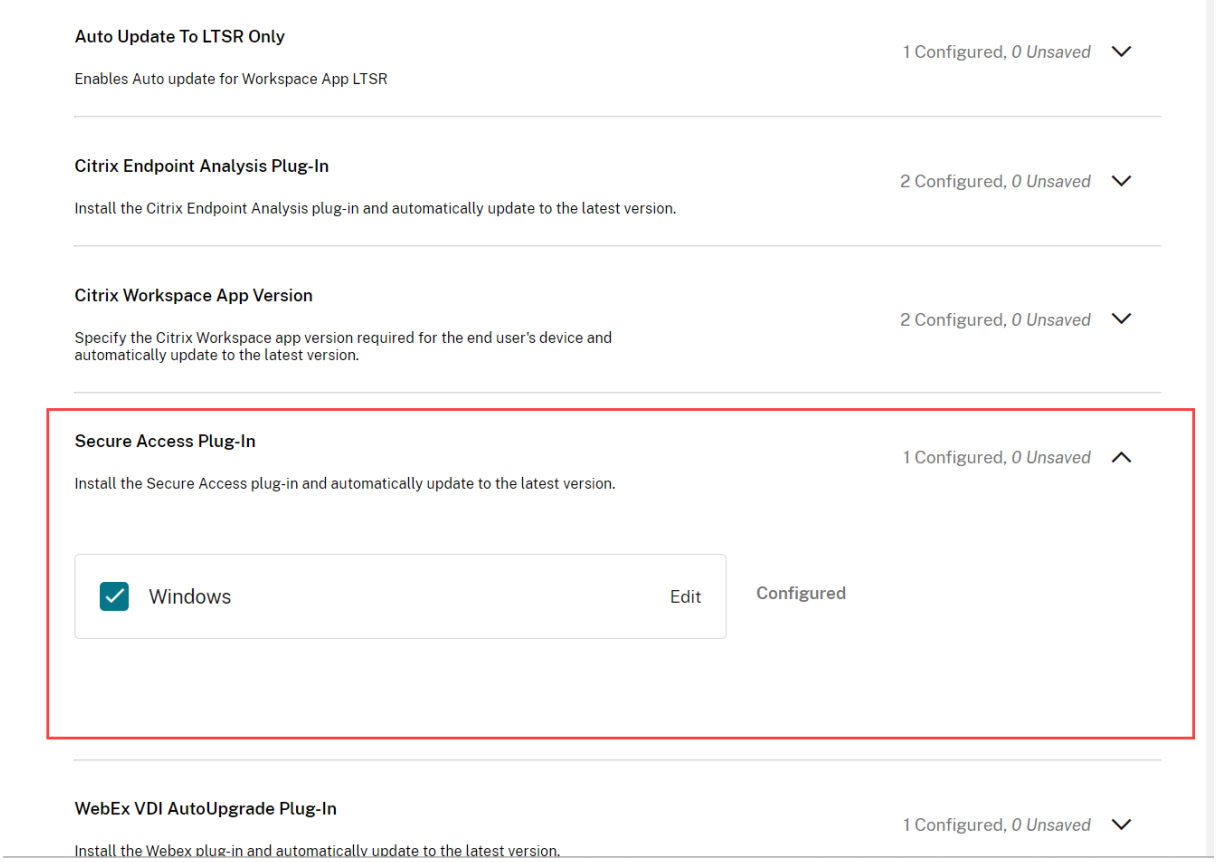
For more information, see Manage Citrix Endpoint Analysis client for Device Posture service.

### 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 AutoUpgrade Plug-in

The Webex App VDI solution optimizes the audio and video for calls and meetings. With GACS, you can manage the Webex VDI Plug-in manager. The Webex VDI Plug-in manager, in turn, installs and

manages the Webex plug-in installed on the end-user's device.

> **Note:**
>
> 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

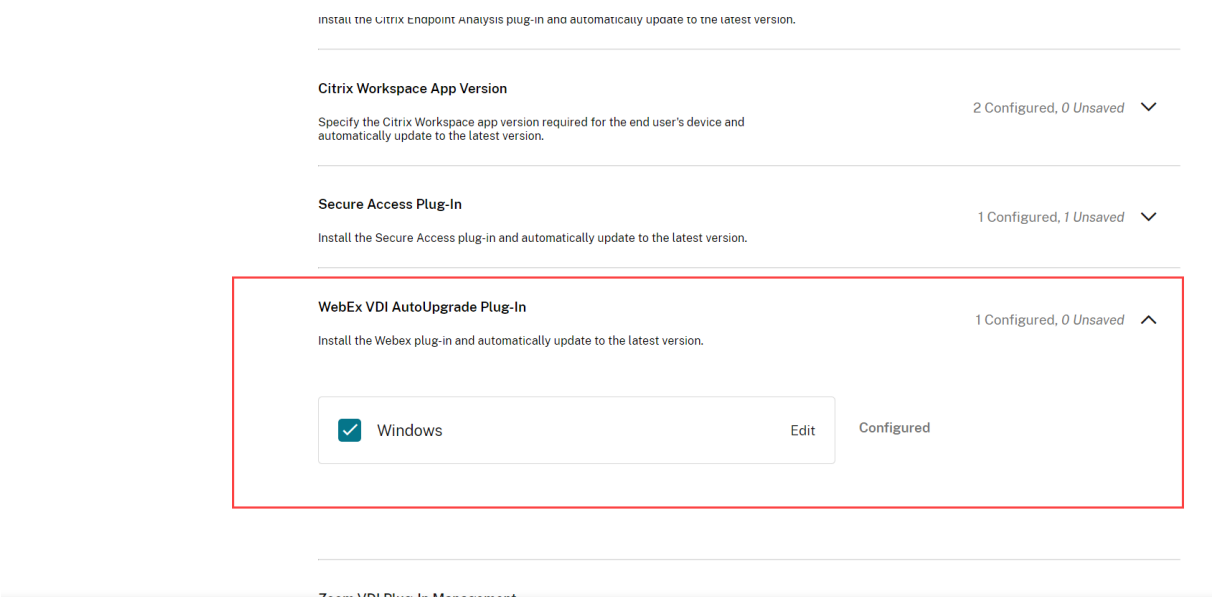
Before proceeding, you must ensure that you've completed the steps listed in the Prerequisites section below.
You can then configure your plug-in settings as described in the **Deployment mode** section.

**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 Autoupgrade 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 AutoUpgradeVDIPluginEn`
   `=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

Once 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 manager 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 steps below:

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:

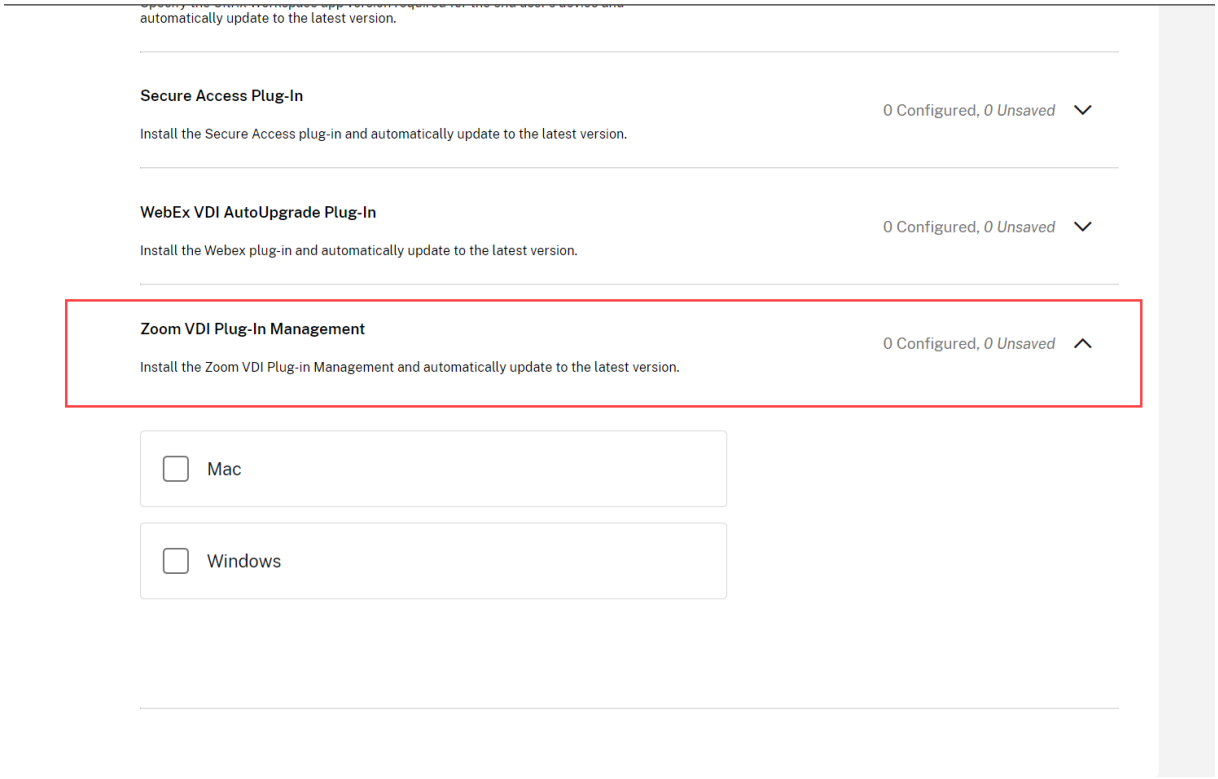
```
- 0— enables the version compatibility check (default)
- 1— disables the version compatibility check
```

### 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 Prerequisites section below.
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 should 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 will be disconnected to install the VDI plugin on the endpoint. Upon clicking **OK**, Zoom would 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 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

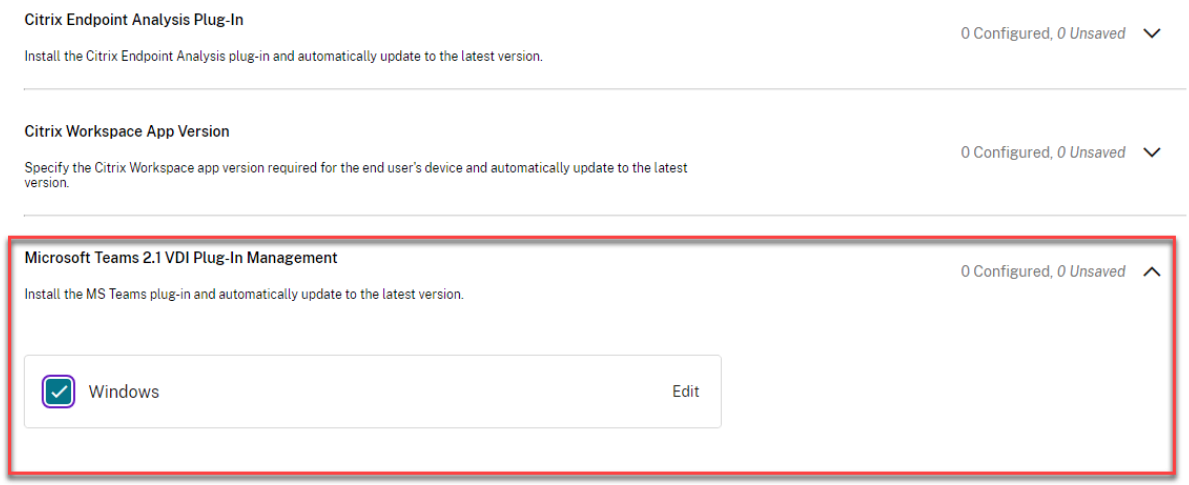
Before proceeding, you must ensure that you've completed the steps listed in the following **Prerequisites** section.

### 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 CVAD 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 Teams.

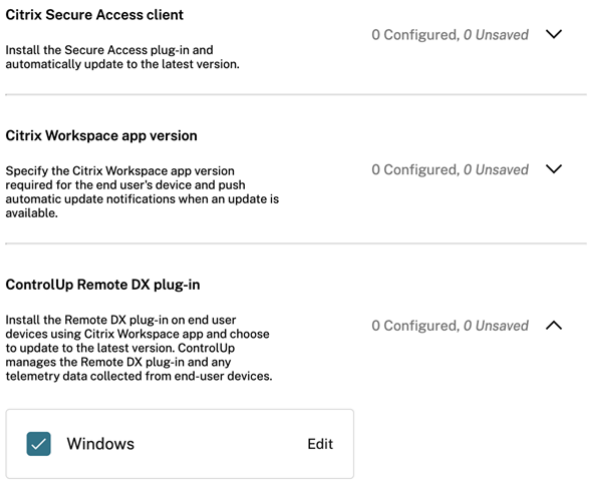
> **Note:**
>
> - Reconnect the session after the successful installation of the plug-in on the end-user device. After that, Microsoft Teams VDI app needs to be restarted twice to enter VDI 2.0 mode.
> - This plug-in is available only on the Windows platform, and it is applicable starting with Citrix Workspace app for Windows version 2405.
> - This plug-in is only applicable to New Teams (Teams 2.x) and not Classic 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 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.
> Telemetry data collection by the RemoteDX plug-in from an end-user's device, if any, is also managed by ControlUp.

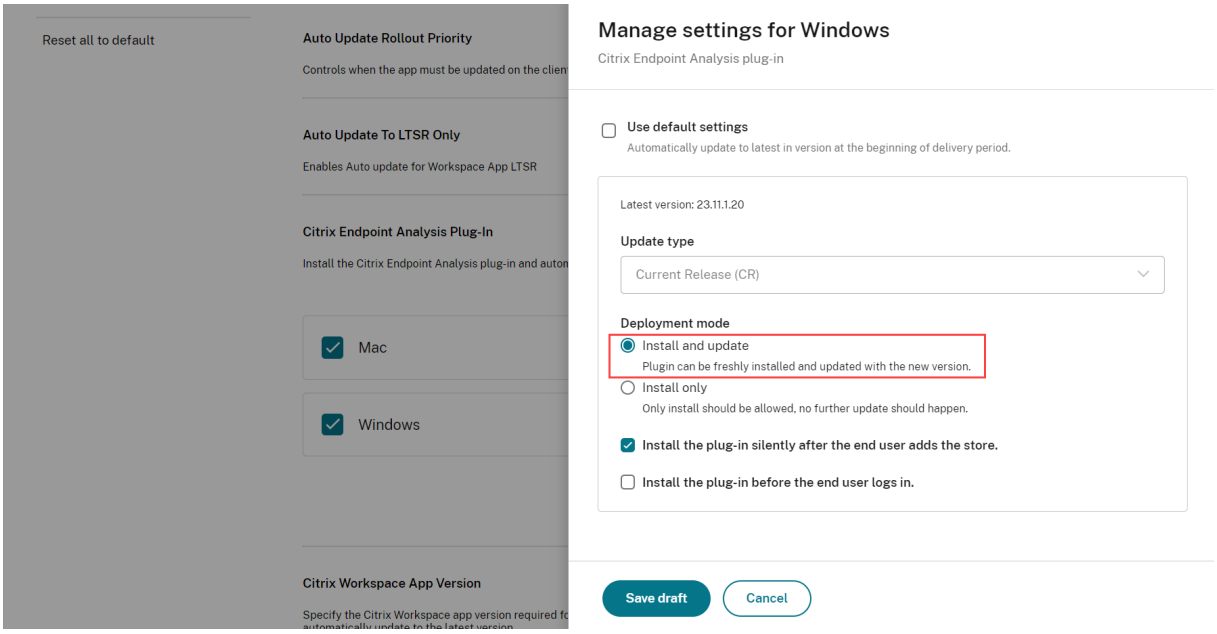
 




## Deployment mode settings

Sign in to your Citrix Cloud account and navigate to **StoreFront Cloud > 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 expand icon to view the applicable platforms. Select the platform that you want to configure the settings for and click **Edit**.

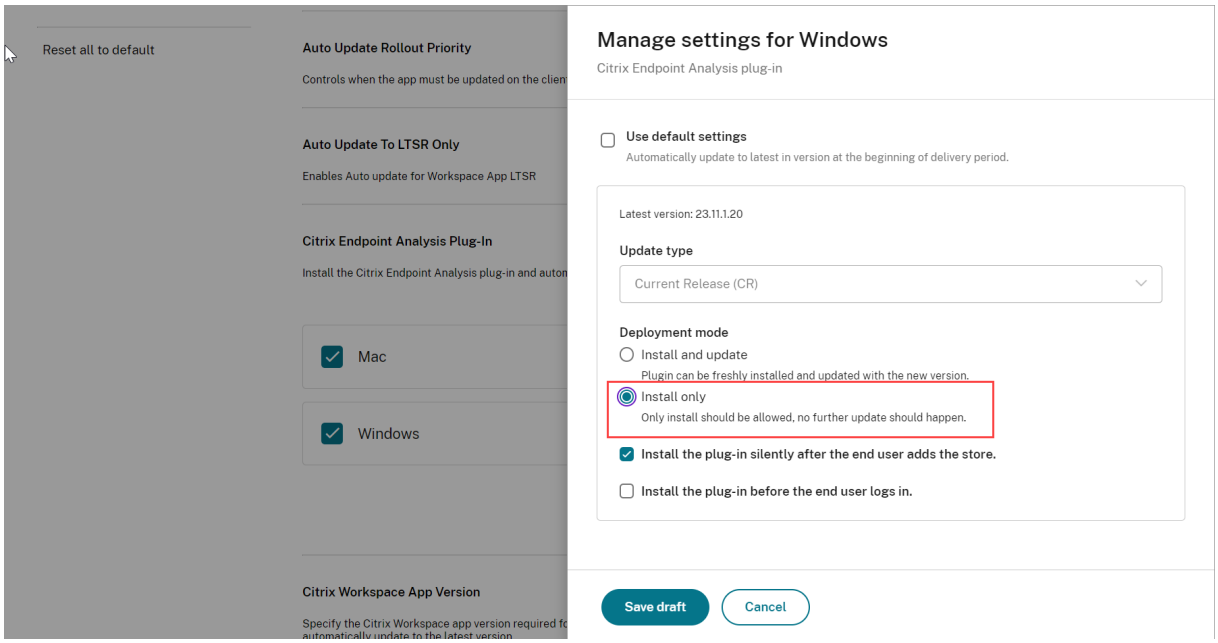
- **Install and update**: Installs the latest version of the plug-in on the end-user's device. It automatically updates the plug-in to the latest version.



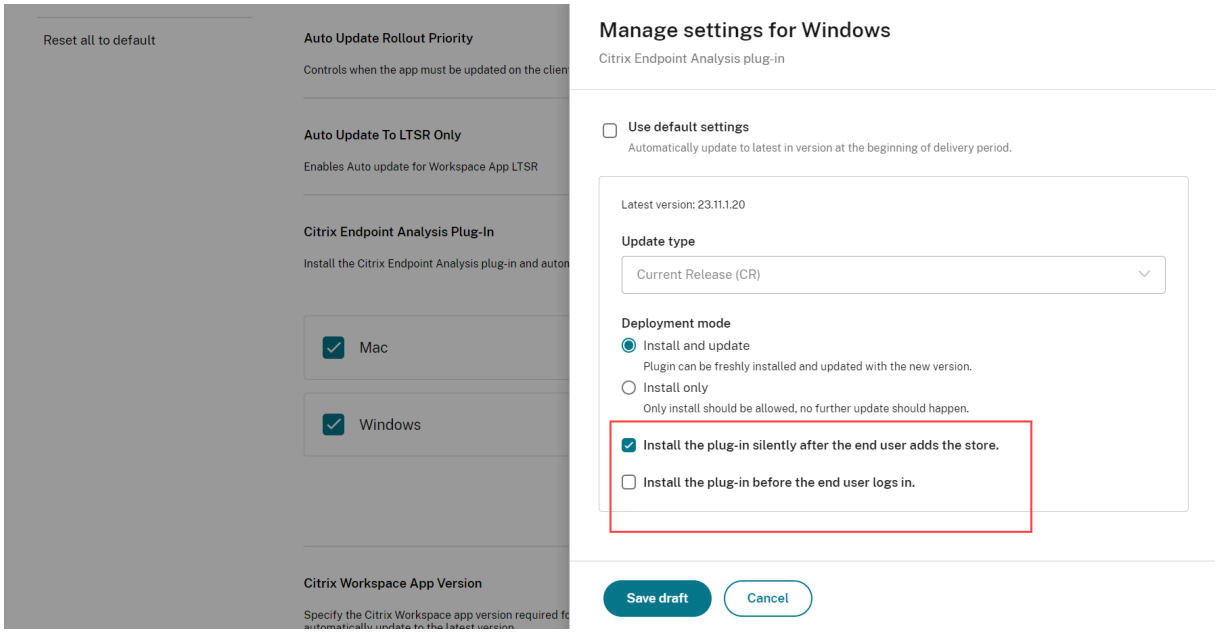

- **Install only**: Installs the latest version of the plug-in on the end-user's device. It does not auto-

update.




After you've selected the deployment mode, you must specify if the plug-in installation or update must require the end-user's intervention. You can select one of the following options.




- **Install the plug-in silently after the end-user adds the store**: The plug-in is installed or updated to the latest version after the end user has added the store. The installation is completed in the background and end users receive a notification once the installation or update is completed. They can sign in and access their stores as usual.
- **Install the plug-in before the end user logs in**: The end user will be unable to sign in to their

Citrix store until the installation is completed. Once the installation is completed, the end users receive a notification. End users are then redirected to authenticate and access the store. Upgrade occurs in regular auto update cycle.

### Delay Group

- **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.

## Manage settings for user group using configuration profile

June 22, 2026

This section explains how to configure settings for user groups using the configuration profile feature in Global App Configuration service (GACS).

> **Note:**
>
> This feature is currently available for cloud stores on Windows, Mac, Linux, Android, and iOS platforms.

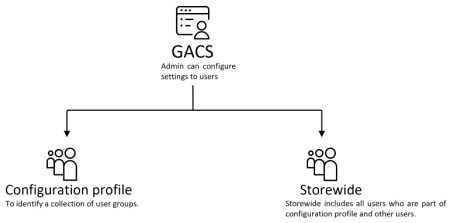
### Introduction to user group and configuration profile

A user group is a collection of users that are created and managed by administrators. Configuring settings for a user group ensures that all users within the user group have the same experience simultaneously. You can create a user group through your organization's identity provider (IdP) by leveraging the AD group information stored in the IdP. For more information on the list of supported identity providers, see Configure Authentication.

A configuration profile is used to identify a collection of user groups and it represents a higher-level abstraction of user groups, with each configuration profile capable of containing multiple user groups. If you need to configure some settings for a particular user groups, you can create a configuration profile and add those user groups to it. You can choose any configuration profile and assign settings to it, so that the experience is applied to all user groups within the configuration profile.

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




## Workflow of Storewide and Configuration profiles

Administrators can configure a setting for users either through Storewide or Configuration profiles. This section explains how the configuration process works in both Storewide and Configuration profiles.

### Storewide

When you configure a setting for Storewide, it takes effect in the following two ways, depending on the context of that setting:

- **For settings available only for Storewide:** Some settings are available only for Storewide. For example, "the web browser for authentication"setting. When you configure such settings, they are applicable to all users, including those within Configuration profiles.
- **For settings available for both Storewide and Configuration profiles:** Some settings are available for both Storewide and Configuration profiles. For example, the "Reconnect apps and desktops"setting. When you configure such settings for Storewide, they are not applied to users assigned to a profile by default. Such settings must also be configured in individual profiles for those settings to take effect.

For more information on configuring a setting for Storewide, see Configure settings for storewide.

### Configuration profiles

When you configure a setting for a Configuration profile, it applies to all users within that Configuration profile.

For more information on configuring a setting for Configuration profiles, see Configure settings for configuration profiles.

## Set Priority

When a user group belongs to multiple configuration profiles, settings from the configuration profile with the highest priority will be applied to that user or user group. The lower the value, the higher

the priority. For more information about setting a priority, see Create a configuration profile and Edit priority.

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

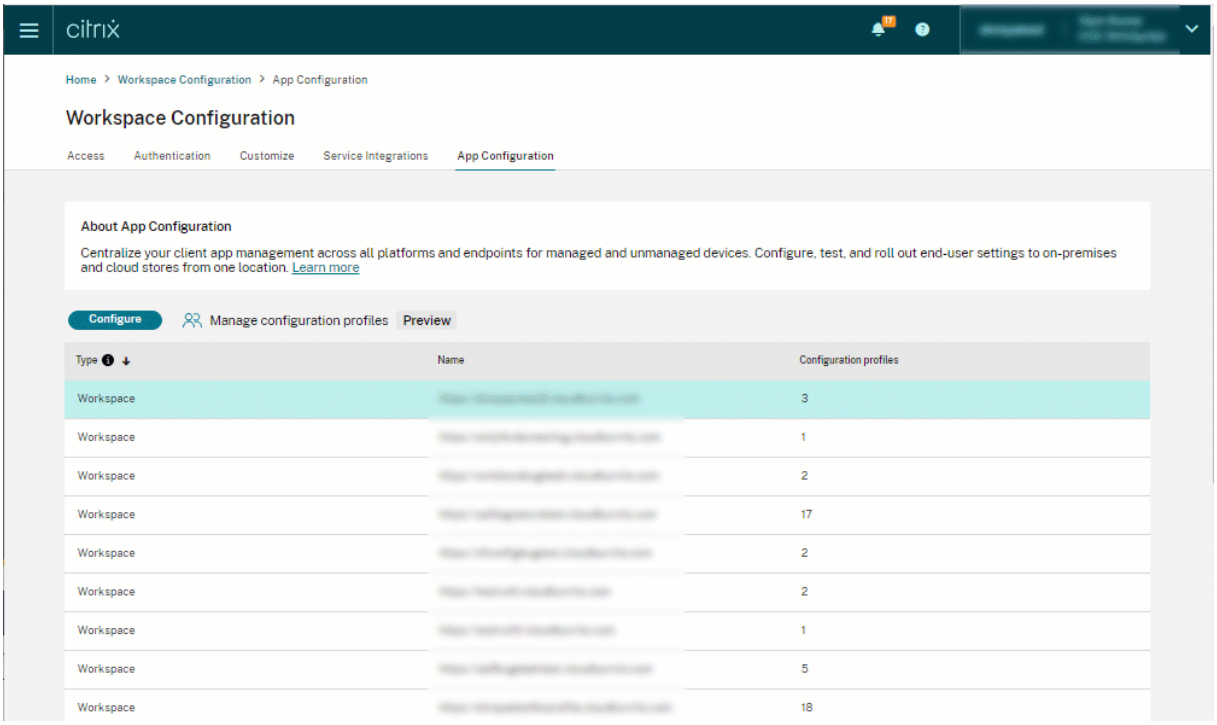
## Create a configuration profile

You can create a configuration profile in two different ways. Either from the **App Configuration** page or from **App Configuration** > **URL Configuration** page.

### Create configuration profile from Citrix® StoreFront Cloud page

1. Sign in to your Citrix Cloud™ account and navigate to **StoreFront Cloud** > **App Configuration**.
2. Click **Manage configuration profiles**.
3. Click **Create** to create a configuration profile.
4. Enter the name, description, and priority of the configuration profile in the **Name**, **Description**, and **Priority** fields respectively.
5. In the **Search for user groups** field, enter a keyword and search the user groups that you want to add into this configuration profile. You can add the desired user groups by clicking the user group from the search list.
6. Click **Save**.

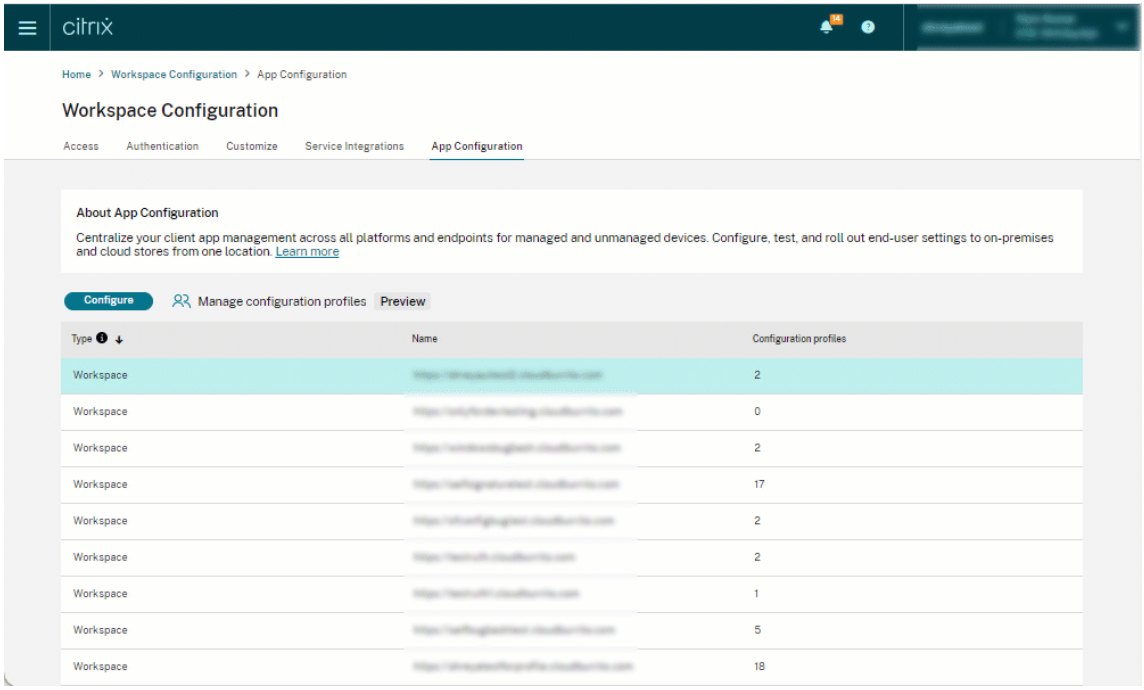



> **Note:**
>
> **Name** and **Priority** are mandatory fields.

### Create configuration profile from URL configuration page

1. Sign in to your Citrix Cloud account and navigate to **StoreFront Cloud** > **App Configuration** > **URL configuration**. You can navigate to the URL configuration page by clicking on the **Configure** button.




2. Click **Manage configuration profiles**, and then click **Create**.

For further instructions, see steps 3 –7 given in Create configuration profile from Citrix® StoreFront Cloud page.

### Edit a configuration profile

1. Navigate to **StoreFront Cloud** > **App Configuration**.
2. Click **Manage configuration profiles**.
3. Select the configuration profile you want to delete from the given list.
4. Click **Edit**.
5. Update the relevant fields, and then click **Save**.

### Edit priority of a configuration profile

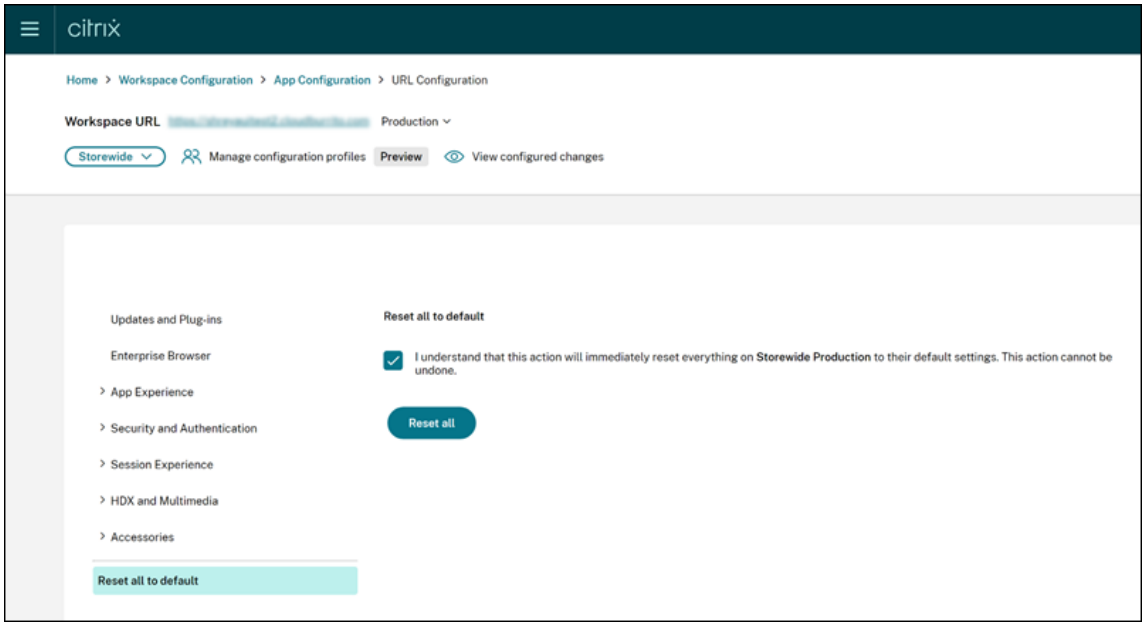
1. Navigate to **StoreFront Cloud** > **App Configuration**.
2. Click **Manage configuration profiles**.
3. Select the configuration profile you want to delete from the given list.
4. Click **Edit priority**.
5. Update the priority value, and click ☒ to update the value or click ☒ to cancel the changes.
6. Click **Close**.

### Delete a configuration 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 **StoreFront Cloud** > **App Configuration**.
2. Click the **Configure** button, and select the appropriate configuration profile from the drop-down list.
3. Click **Reset all to default**.
4. Check the declaration, and click **Reset all**.




> **Note:**
>
> If you haven't configured any settings for the configuration profile, you don't have to reset the settings. So, you can skip steps 2 –4 in that case.

5. Click **Manage configuration profiles**.
6. Select the configuration profile you want to delete from the given list.
7. Click **Delete**.

> **Note:**
>
> You can use the **Edit**, **Delete**, and **Edit priority** options from both **StoreFront Cloud** page and **URL Configuration** page.

### Configure settings for configuration profiles

1. Sign in to your Citrix Cloud account and navigate to **StoreFront Cloud** > **App Configuration** > **URL configuration**.
2. Select the appropriate configuration profile from the drop-down list.
3. Configure relevant settings for the configuration profile.

### Configure settings for storewide

This section describes two scenarios where you have to configure settings only for storewide.

#### Use case 1: Settings that can be configured only for storewide

Some settings cannot have a custom value for user groups. These settings are covered as part of Storewide and appear inactive when accessed within the configuration profile. You can see a warning message with an option to switch to the **Storewide** configuration page.

Alternatively, you can configure the settings for storewide using the following instructions.

1. Navigate to **StoreFront Cloud** > **App Configuration** > **URL configuration**.
2. Select **Storewide** from the drop-down list.
3. Configure relevant settings.

#### Use case 2: Configure settings for remaining users

If you haven't grouped any users under a configuration profile, those remaining users are covered by Storewide. To configure settings for such users, see steps 1 –3 given in Use case 1: Settings that can be configured only for storewide.

> **Note:**
>
> When you configure a setting for both Storewide and a configuration profile, the configuration profile holds the highest priority at the time of applying settings.

## Clone settings across stores, channels, and configuration profiles

June 22, 2026

Clone settings refers to the ability to duplicate settings which are already configured through Global App Configuration service. 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.

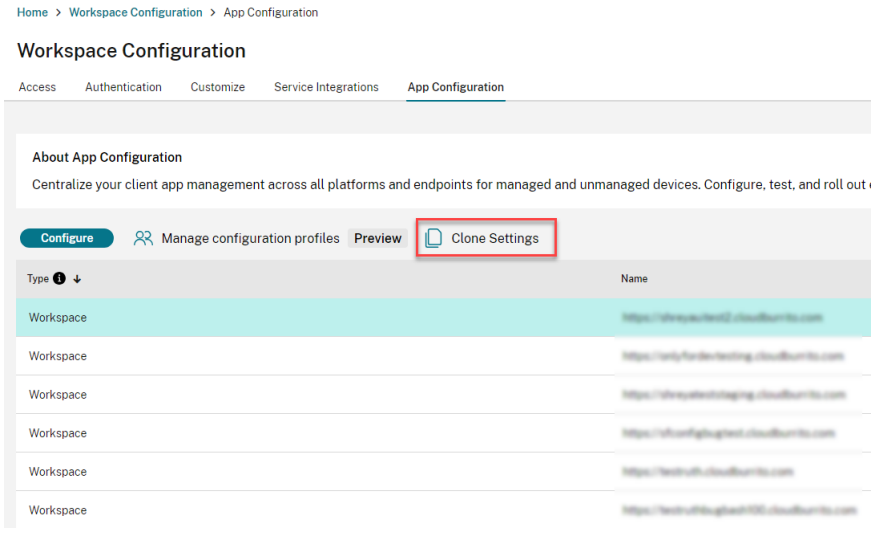
GACS allows cloning of settings in the following scenerios:

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

> **Note:**
>
> - Cloned settings overwrite the existing settings at the destination.
> - Certain storewide-only settings can't be cloned to the configuration profile with From store to a configuration profile option.
> - Cloning between stores is possible only with stores of the same type. Both the source and destination stores need to be either cloud or on-premises stores.

To use this feature, you need to:

1. Navigate to **StoreFront Cloud** > **App Configuration** in your Citrix Cloud™ account.
2. Select the desired store from the given store list, and click the **Clone Settings** option.



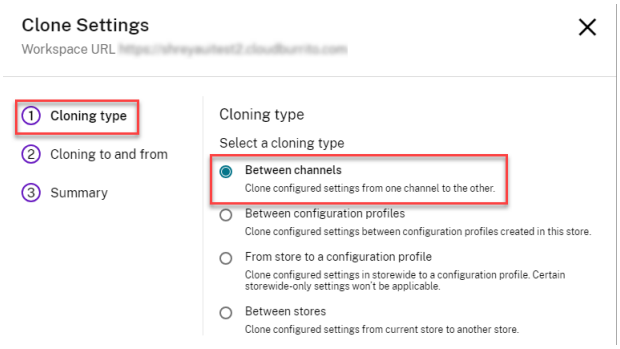

3. Select a cloning type from the **Clone Settings** window, and click **Next**.
4. Select **Cloning to and from** information by selecting the appropriate details from the drop-down list.

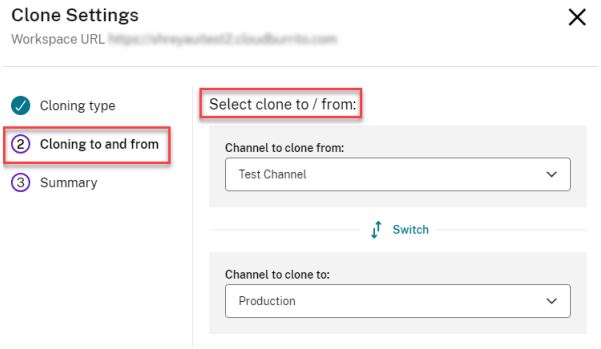
 

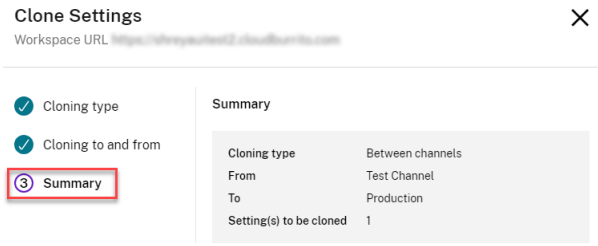
See the following sections for more information about steps 3 and 4.

**Clone settings between channels:**

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

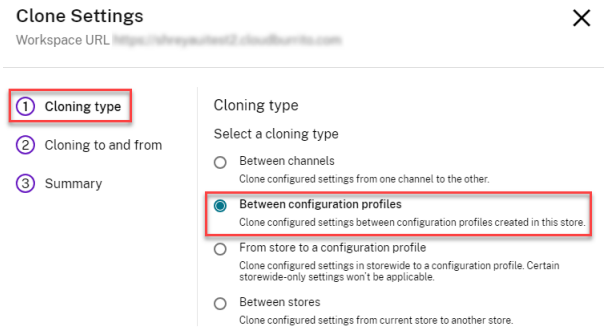


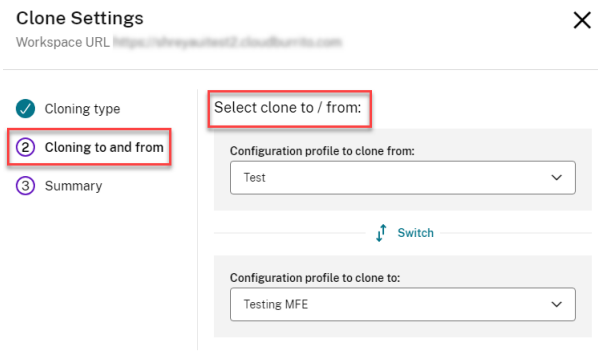



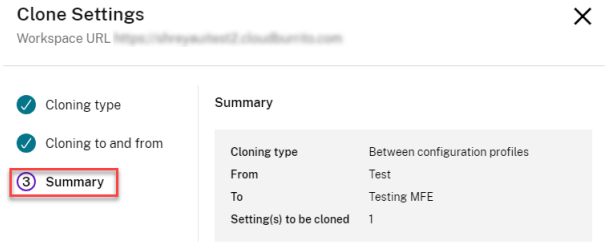

**Clone settings between configuration profiles:**

You can clone the settings between two configuration profiles.



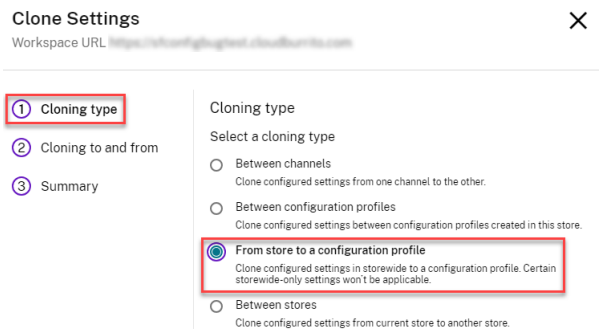

 

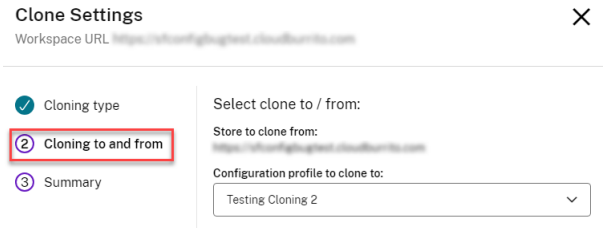


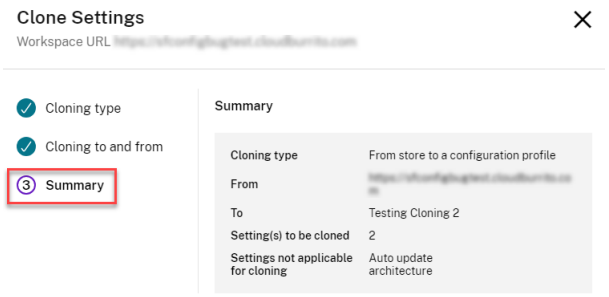

### Clone settings from store to configuration profiles:

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



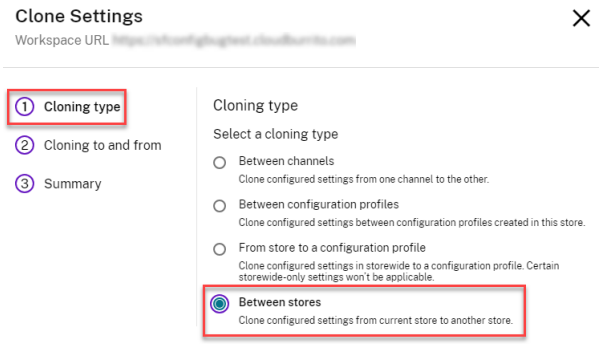



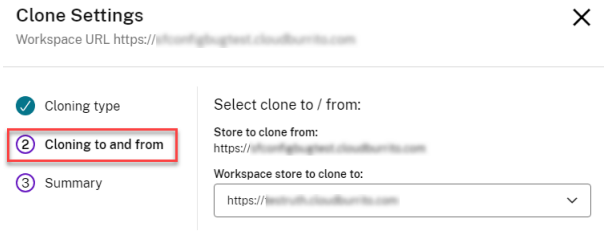

 

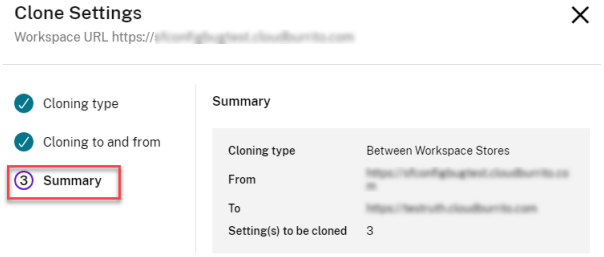



**Clone settings between stores:**

You can clone the settings between stores.

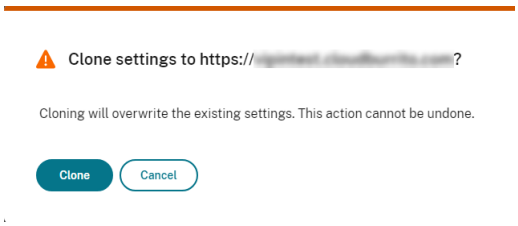


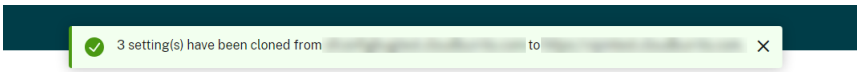




5. Click **Next**.
6. Verify the configured clone settings on the **Summary** page, and click **Clone**.




You can see a notification following the successful cloning.




## Manage settings for hybrid launch

June 22, 2026

Citrix Workspace app enables its management via Global App Configuration service (GACS) 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, GACS 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 behaviour

This section describes Citrix Workspace app behaviour 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 GACS settings are changed during the active session. | GACS settings are applied during the next session launch. |

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

### Cloud store support

To get started, administrators need to enable in-memory hybrid launches. This means 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 store, see store PowerShell documentation.

> **Note:**
>
> Hybrid launch via Citrix Web Extension isn't currently supported.

To enable this feature, submit a request using this enablement form.

### On-Premises Support

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

- Whitelist GACS endpoint
- Configure registration tool
- Enable in-memory hybrid launches
- Minimum supported version of StoreFront is 2503.

> **Note:**
>
> Hybrid launch via Citrix Web Extension isn't currently supported.

### Whitelist GACS endpoint

For more information, see Prerequisites.

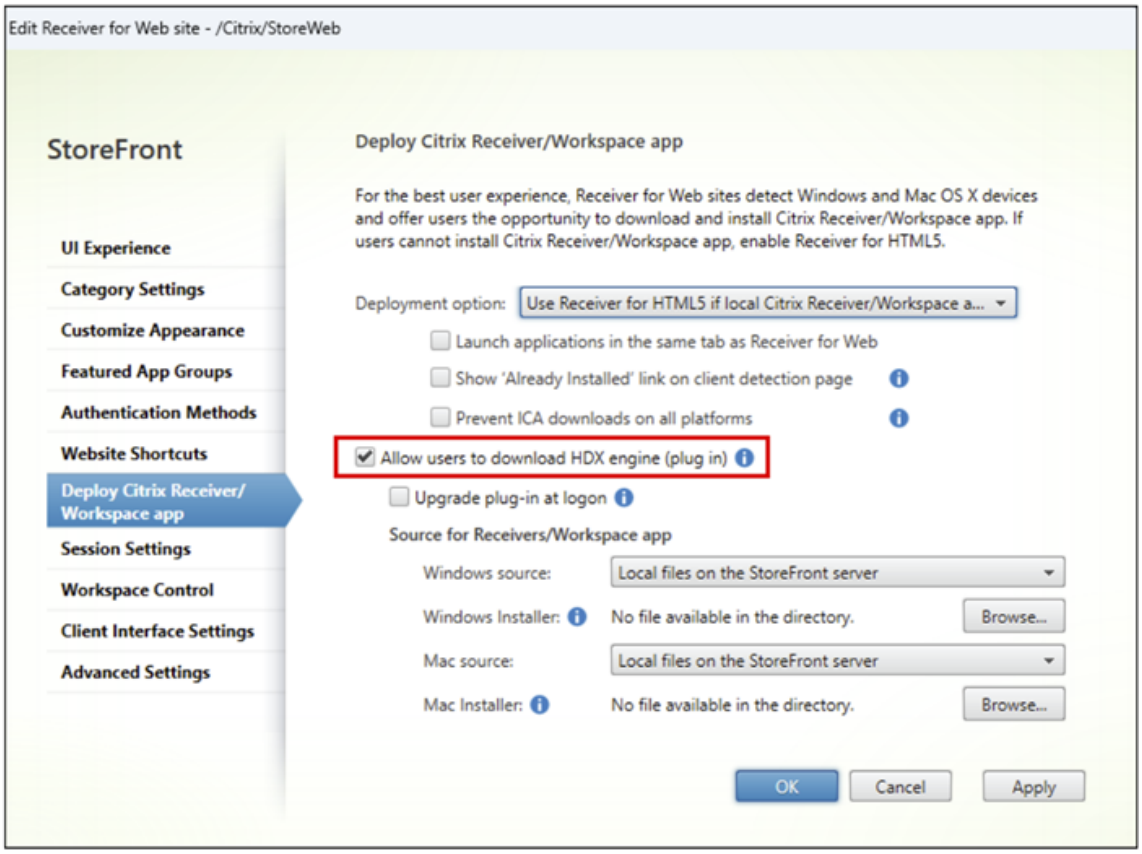
### Configure registration tool

For more information, see Configure registration tool.

### Enable in-memory hybrid launches

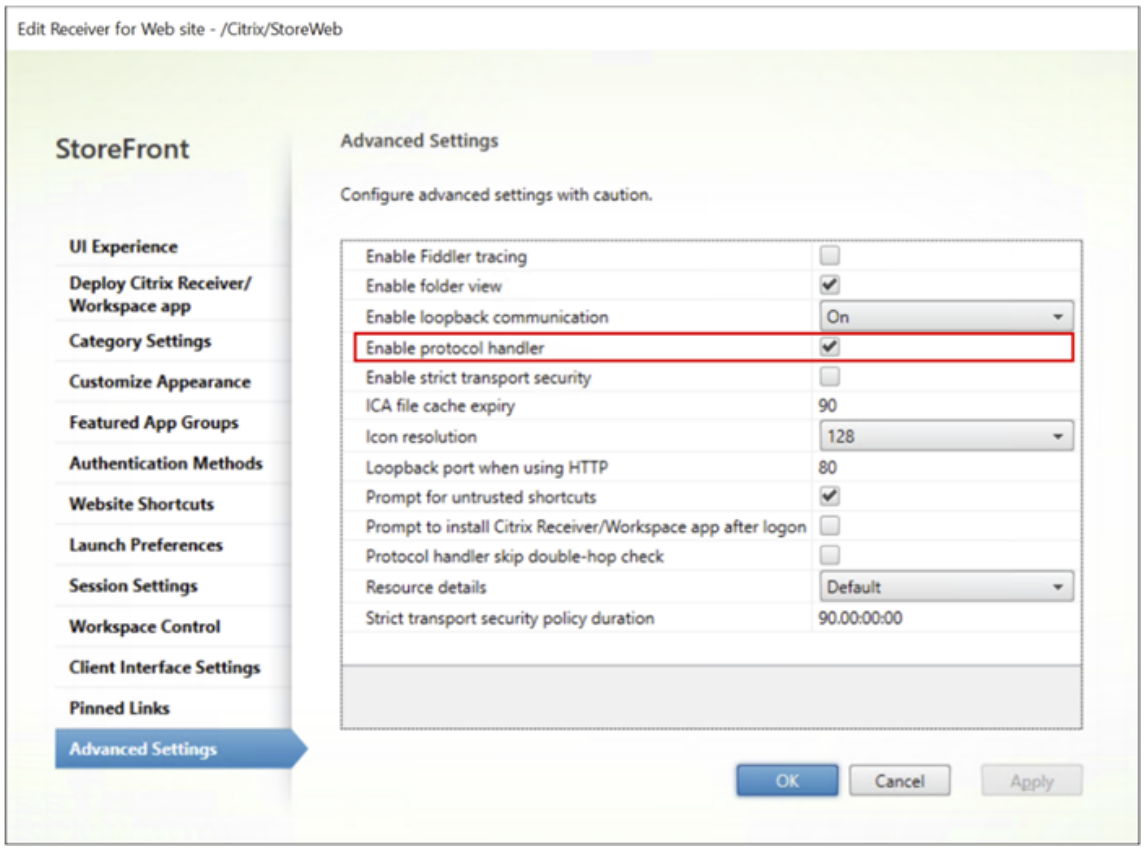
To enable in-memory hybrid launches, do the following steps:

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.




## Configure settings for custom domain

June 22, 2026

You can apply the Global App Configuration service (GACS) settings to `custom domain URLs` in addition to `cloud.com domain URLs`. After you enable this setting in the GACS 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.

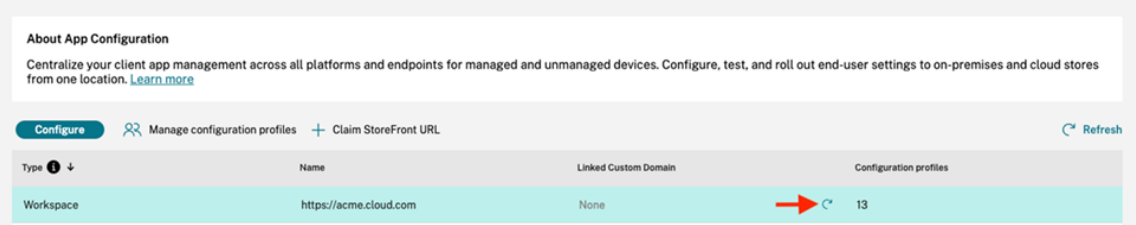
### Workflow to enable settings for custom domain

To enable Global App Configuration service settings for custom domains, perform the following:

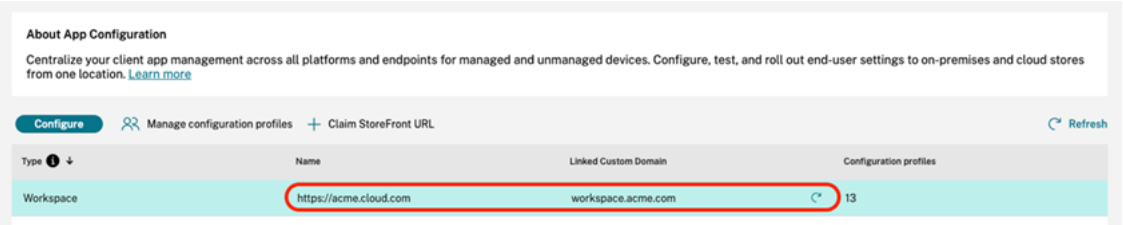
1. Navigate to **StoreFront Cloud** > **App Configuration**.
2. Locate the **Linked Custom Domain** option for each store URL.

3. Click **refresh** icon in the **Linked Custom Domain** column, if a custom domain is configured for the store 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:

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

### Compatibility

The following Citrix Workspace app versions support this feature:

- **Windows:** Version 2503.10 or later
- **Mac:** Version 2503 or later

## Citrix® StoreFront Cloud security overview

June 22, 2026

### User Authentication

Citrix® StoreFront Cloud can be configured to use a wide range of authentication methods. For more details see Configure authentication.

To configure session timeouts, see Store access.

### Client connectivity

Clients must connect to their store using HTTPS with TLS 1.2 or higher. For minimum client versions and network connectivity requirements, see system requirements.

Store websites set HTTP Strict Transport Security headers to require that web browsers only use HTTPS.

### App protection

You can use App protection to prevent screen capture and screen loggers. When using a web browser, this requires Citrix web extensions.

### More information

- Secure Deployment Guide for the Citrix Cloud Platform: This guide provides an overview of security best practices when using Citrix Cloud and describes the information Citrix Cloud collects and manages. This guide also contains links to comprehensive information about the Citrix Cloud Connector.
- Technical security overview for Citrix DaaS.
- Citrix Trust Center: Provides the latest information on our approach to security, privacy, and compliance.