Citrix Workspace

Contents

Citrix Workspace Overview

February 16, 2024

Citrix Workspace is a digital workspace solution that delivers secure and unified access to apps, desktops, and content (resources) from anywhere, on any device. The resources can be any of the following:

- Citrix DaaS
- Content apps
- Local and mobile apps
- SaaS and Web apps
- Browser apps

How Citrix Workspace works

Citrix Workspace aggregates and integrates Citrix Cloud services, enabling unified access to all the resources available to your end-users (subscribers) in one resource location. End users of Citrix Workspace are called subscribers because you "subscribe"employees to the services you make available to them through their workspaces.

For an overview of the services available through Citrix Workspace, see Cloud-hosted services through Citrix Workspace.

Subscribers see a complete, unified view of each resource you make available to them through these services in the Citrix Workspace user interface (UI). For more information on the subscriber experience of the Citrix Workspace UI, see Manage your workspace experience.

Subscribers access the services that you configure and enable in **Workspace Configuration** either through the browser with the Workspace URL, or through the Citrix Workspace app, which replaces Citrix Receiver. For more information on how users access their workspaces, visit Workspace access.

Subscribers authenticate to their workspaces using the primary identity provider that you configure in **Identity and Access Management** and then enable in **Workspace Configuration**. The subscriber is then automatically authenticated to each cloud-hosted service purchased for Citrix Workspace. It helps increase security and reduces usability challenges. For more information on configuring Workspace authentication, visit Secure workspaces.

Get started overview

Citrix Workspace is set up through the **Citrix Cloud console**, in which there's an **Identity and Access Management** administration screen and a Citrix Workspace management interface called **Workspace**

Configuration. Getting started with Citrix Workspace involves the following tasks.

1. Verify that you're set up to implement Citrix Workspace in the **Citrix Cloud console**, where you:
    - Onboard to cloud-based services.
    - Assemble your deployment team.
    - Configure your infrastructure and resources.
2. Define identity providers and accounts in **Identity and Access Management** for:
    - Citrix Cloud administrators.
    - Citrix Workspace subscribers.
3. Configure your workspaces in **Workspace Configuration**, including:
    - Internal and external access.
    - Integrating services that you configured in the Citrix Cloud console into your workspaces.
    - Customizing the workspace appearance and the subscriber experience once they sign in.

Beyond this basic setup, you have other security, privacy, and optimization options to choose from. The most common are:

- Configure single sign-on (SSO) to DaaS in Citrix Workspace with the Citrix Federated Authentication Service (FAS).

> **Note**
>
> FAS is typically adopted if you're using a federated authentication method, such as Okta or Azure Active Directory.

For an overview of the tasks and the information needed as you progress in your deployment, see Get started with Citrix Workspace. Each step guides you through the Citrix Cloud console for tasks like configuring your identity provider. The walkthrough also provides quick access to technical information needed for assembling your deployment team, and configuring your infrastructure and resources.

Cloud-hosted services through Citrix Workspace

Subscribers use Citrix Workspace to access the resources provided by cloud-hosted services. Existing Citrix Cloud customers can transition to the full digital workspace experience by taking these services with them into the Citrix Workspace solution.

This section describes the main cloud-hosted services that can be enabled for Citrix Workspace, depending on your entitlements. For information on how to configure and enable access to your purchased services, visit Get started with Citrix Workspace. For a complete description of each Citrix Workspace edition and included features, see the Citrix Workspace Feature Matrix.

Citrix DaaS

Citrix Workspace is the multitenant, cloud-hosted access point to Citrix DaaS. To set up the Citrix DaaS, follow the steps outlined in Citrix DaaS.

If you're an on-premises Virtual Apps and Desktops customer, there are different options for accessing your resources through Citrix Workspace. The option you choose depends on two factors. The first factor is whether you want to migrate fully to the cloud or adopt a hybrid solution. The second factor is whether you plan to allow external access. For more information on these options, visit Deliver DaaS with Citrix Workspace.

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

Citrix Secure Private Access (formerly **Secure Workspace Access** and the **Access Control Service**) provides single sign-on (SSO) to Web and SaaS apps that are integrated into Workspace. The service also allows you to manage access permissions and control policies. It helps sanction appropriate levels of access to enterprise-hosted web apps based on the subscriber's credentials.

For more information on the benefits of the **Citrix Secure Private Access** service, visit Tech Brief: Secure Private Access.

Citrix Gateway service

The **Citrix Gateway** service (formerly the **NetScaler Gateway Service**) is used with **Citrix Secure Private Access** for a fully cloud-hosted environment, managed by Citrix.

The **Citrix Gateway** service delivers a unified experience to SaaS apps, and Virtual Apps and Desktops, by providing external connectivity to workspaces based on an advanced policy infrastructure.

Follow the steps to set up the Citrix Gateway service, then test and share the Workspace URL with your subscribers to give them remote access. For more information on configuring SaaS apps within the Citrix Gateway service, see Support for Software as a Service Apps.

Citrix Remote Browser Isolation service

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

To give subscribers access to a remote isolated browser, set up Remote Browser Isolation. After that, test and share the Workspace URL with your subscribers.

Citrix Endpoint Management

Citrix Endpoint Management allows you to manage device and app policies with strict security for identity, devices, apps, data, and networks. Integration with Citrix Workspace differs for new and existing customers. For more information on integrating Endpoint Management with Citrix Workspace, visit Integration with Citrix Workspace experience.

Citrix Analytics

The **Citrix Analytics** service gathers and provides insights on all your Citrix Workspace subscribers. There are different Citrix Analytics offerings available to you depending on your entitlements. The offerings include **Citrix Analytics for Security**, **Citrix Analytics for Performance**, and **Citrix Analytics (Usage)**. To learn more about these services, visit Citrix Analytics.

What's New

October 26, 2023

Citrix aims to deliver new features and updates to Citrix Workspace customers when they are available. Initial releases are applied to Citrix internal sites and are gradually applied to customer environments.

For details about the Service Level Agreement for cloud scale and service availability, see the Citrix Cloud Service Level Agreement. To monitor service interruptions and scheduled maintenance, see the Service Health Dashboard.

What's new in Citrix Workspace

Stay informed about the latest enhancements and updates in Citrix Workspace to use the full potential of our technology. Maximize your user's productivity and enhance the quality of their interactions by incorporating timely updates from Citrix Workspace.

- What's new in Workspace Platform
- What's new in Workspace User Interface
- What's new in Global App Configuration Service

Citrix Workspace app on various platforms

Learn more about the new features and enhancements in **Citrix Workspace App** for your favorite platforms using the following links.

- Android
- ChromeOS
- HTML5
- iOS
- Linux
- Mac
- Microsoft Teams
- Windows
- Windows Store

Also, see what's new in Citrix Enterprise Browser.

What's new in Workspace platform

February 22, 2024

Citrix aims to deliver new features and updates to Citrix Workspace customers when they're available. New releases provide more value, so there's no reason to delay updates.

This process is transparent to you. Initial updates are applied to Citrix internal sites only and are then applied to customer environments gradually. Delivering updates incrementally maximizes product quality and availability.

For details about the Service Level Agreement for cloud scale and service availability, see the Citrix Cloud Service Level Agreement. To monitor service interruptions and scheduled maintenance, see the Service Health Dashboard.

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.

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 multiple Workspace URLs.

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.

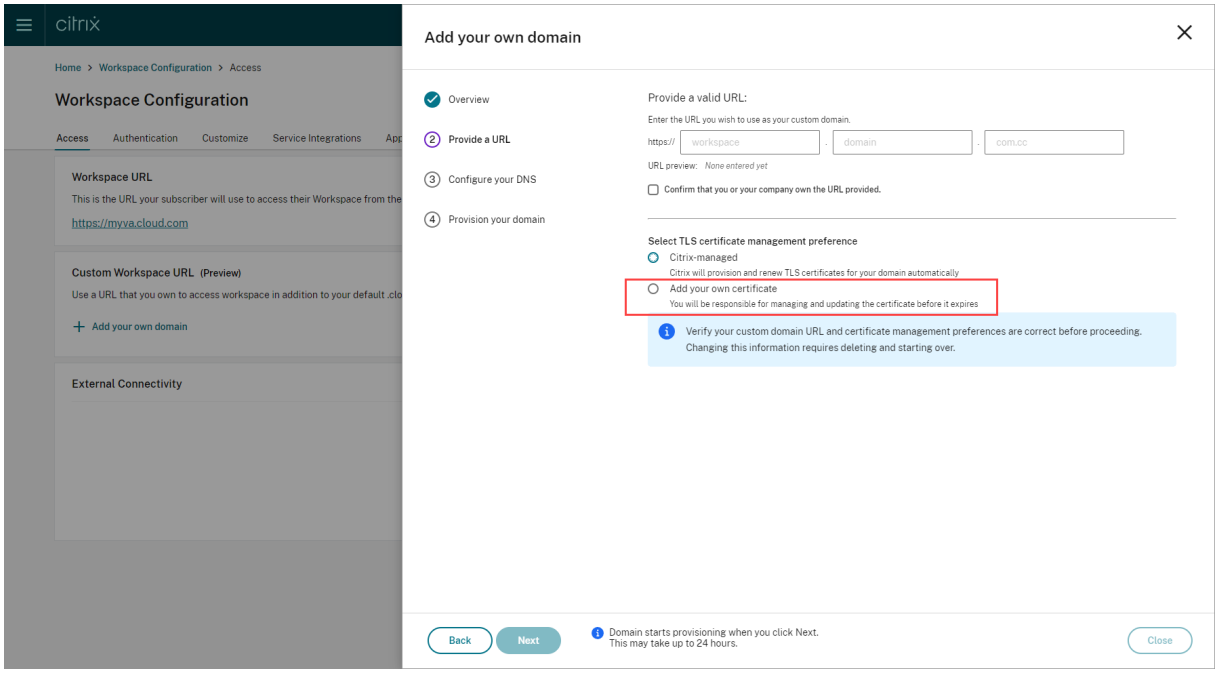
Aug 2023

Add your own TLS certificate for custom domain (Preview)

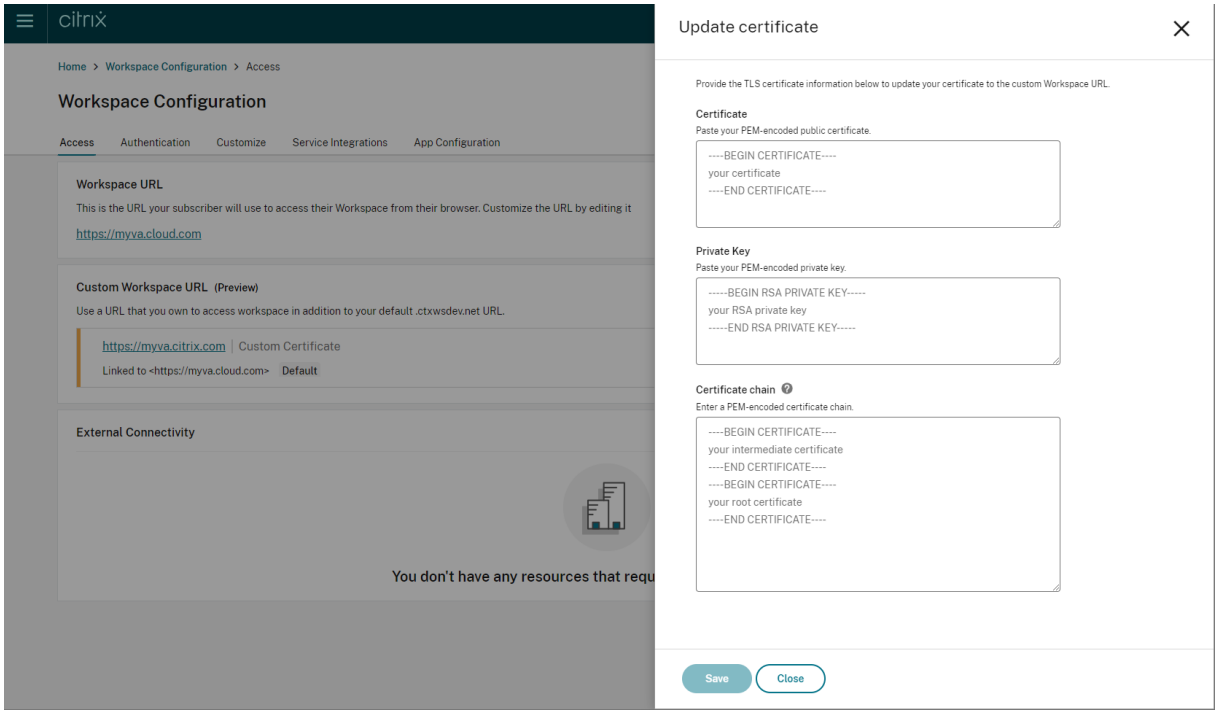
You can now upload your own TLS certificate for authentication while configuring a custom Workspace URL. Before uploading a certificate, ensure that the certificate fulfills the following conditions.

- 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.

> **Note:**
>
> You can provide feedback for this preview feature using the attached Podio form.

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 subscribers 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 subscribers to stay signed in to Workspace without being prompted to sign in every time they access their workspace. When signing in through Workspace app, subscribers consent to stay signed in. Subscribers remain signed in during the reauthentication period as long as they're using their apps and desktops. For more information about this feature, see Set a reauthentication period for Citrix 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 Customize security and privacy policies.

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. For more information, see Create a unified user sign-in flow.

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 **Workspace Configuration**. 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 subscriber license agreement policy: You can present subscribers 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 subscribers to stay signed in to Workspace without being prompted to sign in every time they access their workspace. When signing in through Workspace app, subscribers consent to stay signed in. Subscribers 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 subscribers now supports custom themes that you can assign to different user groups. Create, customize, and prioritize themes so subscribers 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: Subscribers can change their domain password from within Citrix Workspace. Administrators can also provide password guidance to subscribers for creating valid complex passwords in accordance with their organization's password policy. For more information, see Allow subscribers 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.

October 2020

FedRAMP Ready: Citrix Workspace is FedRAMP Ready when deployed in Citrix Cloud Government. FedRAMP is a program that promotes security standards for cloud services used by US government organizations. US government organizations that require FedRAMP Ready cloud services can now use Citrix Workspace and Citrix DaaS services to deliver DaaS. For more information, see Citrix Cloud Government.

May 2020

Get Started with Citrix Workspace guide: Citrix Workspace now includes a step-by-step walk-through 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.

What's new in Workspace user interface (UI)

April 30, 2024

The following sections list the new features in current and earlier releases for Workspace UI.

> **Note:**
>
> - For more information on the new UI, see New Workspace user interface.
> - For more information on Activity Manager, see Activity Manager.

What's new in 24.18

This release addresses areas that improve overall performance and stability.

Fixed issues

This release addresses areas that improve overall performance and stability.

Known issues

There are no known issues in this release.

Earlier releases

This section provides information on new features and fixed issues in the earlier releases that we support.

24.17

This release addresses areas that improve overall performance, stability, and feature enhancements.

24.15

This release addresses areas that improve overall performance, stability, and feature enhancements.

24.14

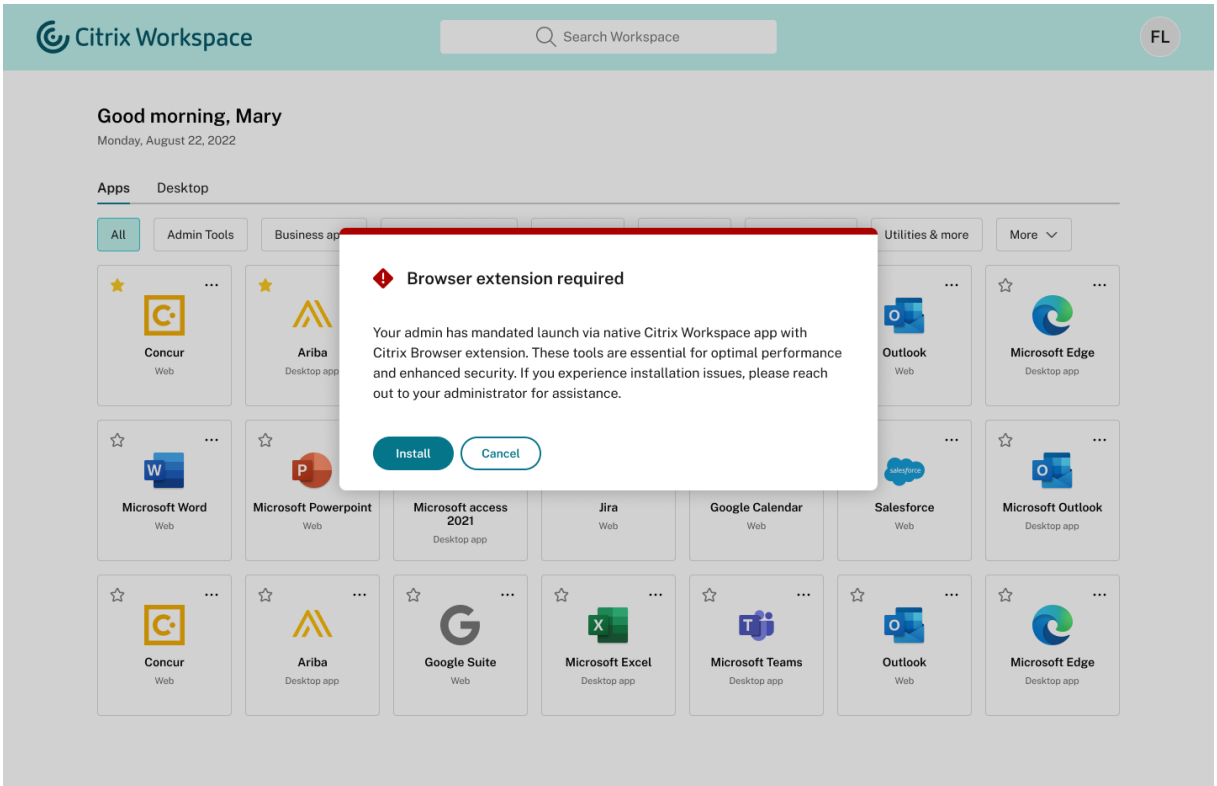
This release addresses areas that improve overall performance, stability, and feature enhancements.

24.13

This release addresses areas that improve overall performance, stability, and feature enhancements.

24.12

Manage installation prompt for Workspace Web extension (Preview) 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.

> **Note:**
>
> You can sign up for this preview feature using the attached Podio form.

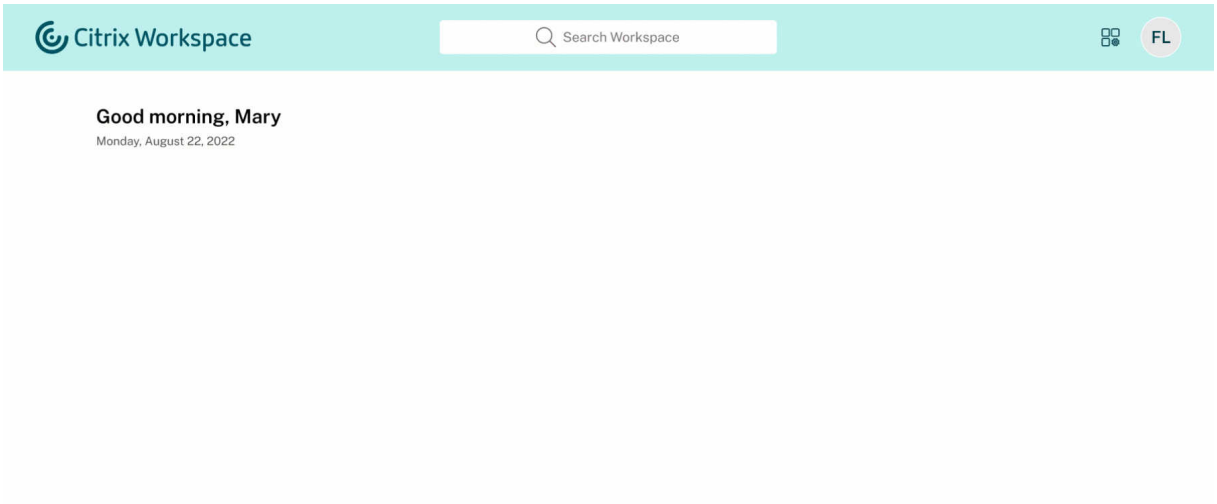
Fixed issues This release addresses areas that improve overall performance and stability.

Known issues There are no known issues in this release.

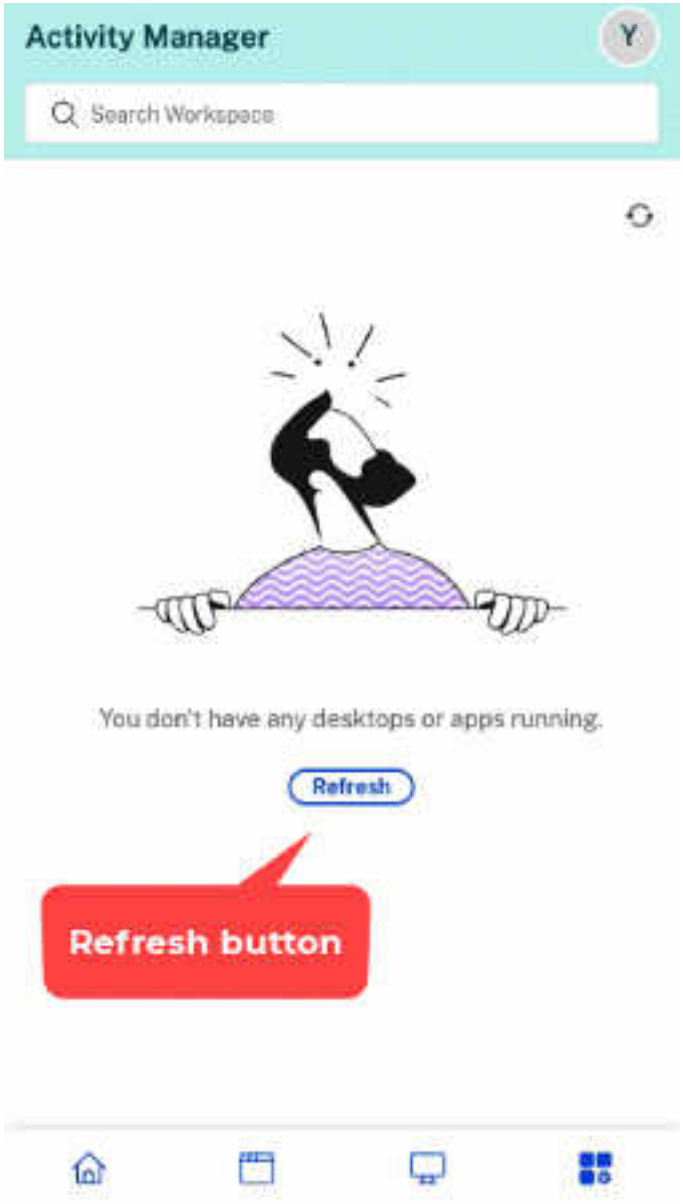
24.11

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:



Fixed issues This release addresses areas that improve overall performance and stability.

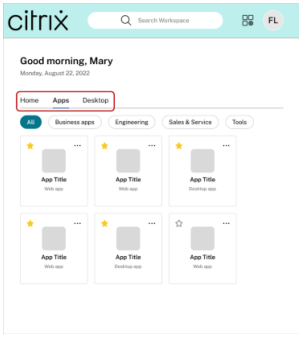
Known issues There are no known issues in this release.

24.10

This release addresses areas that improve overall performance, stability, and feature enhancements.

24.9

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 Workspace visual and layout improvements.

Fixed issues There are no fixed issues in this release.

Known issues There are no known issues in this release.

24.8

This release addresses areas that improve overall performance, stability, and feature enhancements.

Support for Finnish language: Citrix Workspace UI is now available in the Finnish language.

24.7

This release addresses areas that improve overall performance, stability, and feature enhancements.

24.6

This release addresses areas that improve overall performance, stability, and feature enhancements.

24.5

This release addresses areas that improve overall performance, stability, and feature enhancements.

24.4

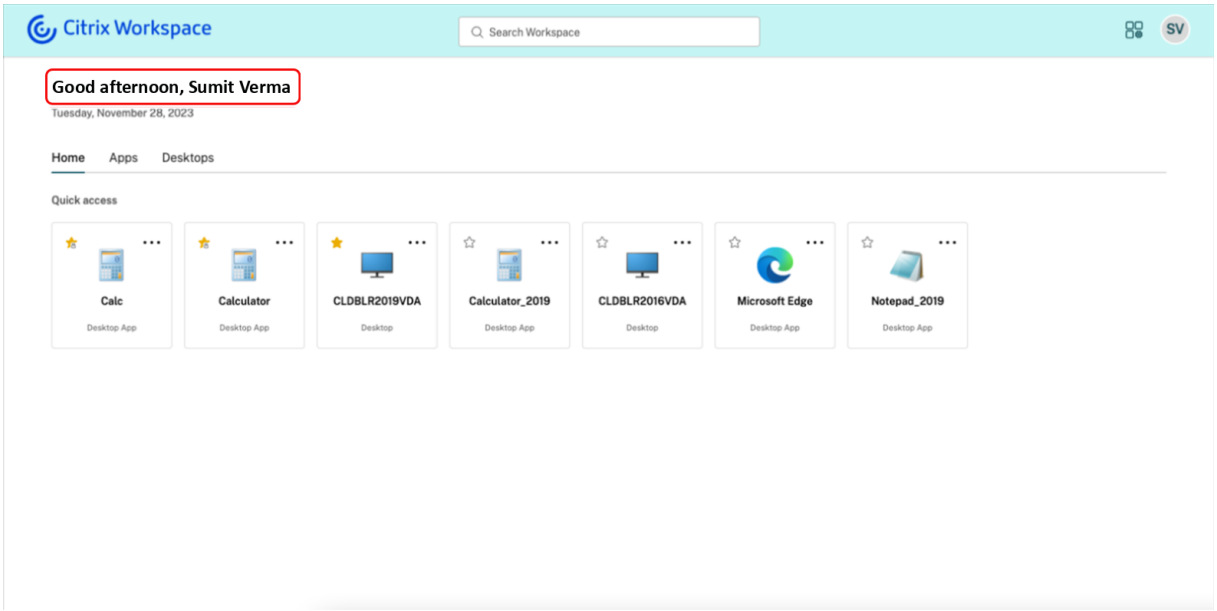
This release addresses areas that improve overall performance, stability, and feature enhancements.

23.49

This release addresses areas that improve overall performance, stability, and feature enhancements.

23.48

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

Fixed issues This release addresses areas that improve overall performance and stability.

23.46

This release addresses areas that improve overall performance, stability, and feature enhancements.

23.45

This release addresses areas that improve overall performance and stability.

Fixed issues

- Google Search indexing has been removed from Citrix Web to prevent internal 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.

23.44

This release addresses areas that improve overall performance, stability, and feature enhancements.

23.43

This release addresses areas that improve overall performance and stability.

Fixed issues This release addresses areas that improve overall performance and stability.

23.42

This release addresses areas that improve overall performance and stability.

Fixed issues This release addresses areas that improve overall performance and stability.

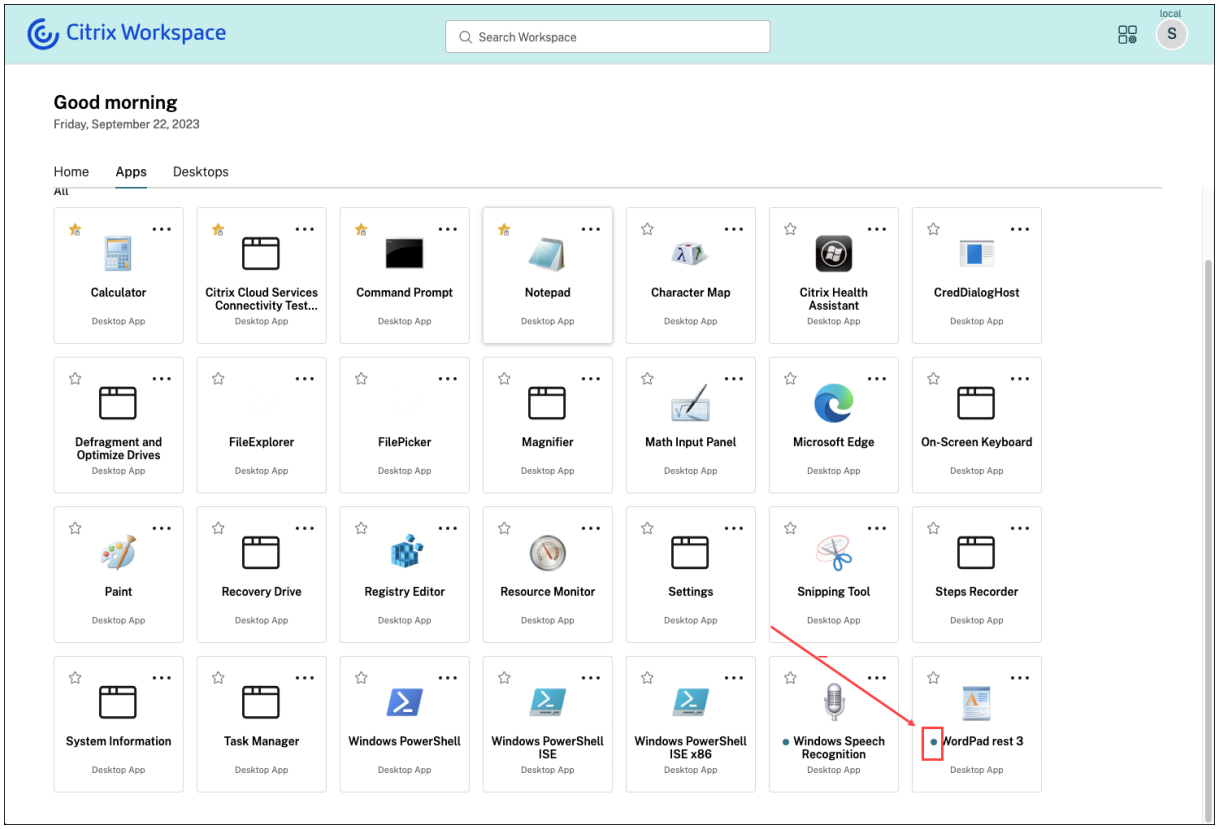
23.41

This release addresses areas that improve overall performance and stability.

Fixed issues This release addresses areas that improve overall performance and stability.

23.40

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.



Fixed issues This release addresses areas that improve overall performance and stability.

23.39

This release addresses areas that improve overall performance and stability.

Fixed issues This release addresses areas that improve overall performance and stability.

23.38

This release addresses areas that improve overall performance and stability.

Fixed issues This release addresses areas that improve overall performance and stability.

23.37

New Workspace UI - General Availability 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 New Workspace UI.

> **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 - General Availability 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**. For more information, see Enable Activity Manager.

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

Following actions can be performed for active apps and desktops.

- **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.

Activity Manager also enables end users to interact with their disconnected apps and desktops. Ensure that you have upgraded to the latest DDC version(115). For more information, see Disconnected apps and desktops.

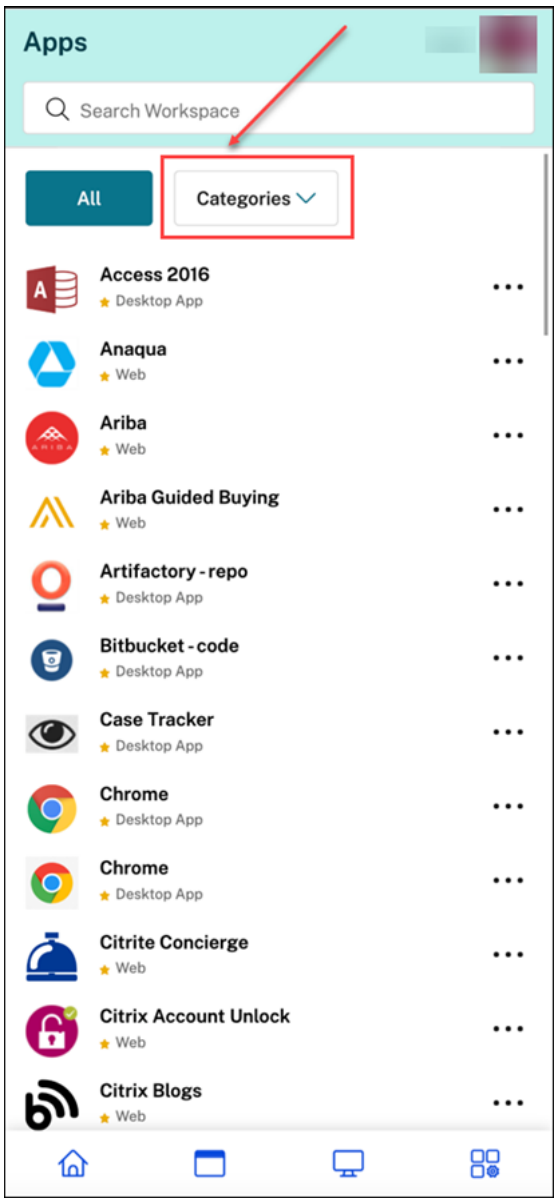
Fixed issues This release addresses areas that improve overall performance and stability.

Known issues

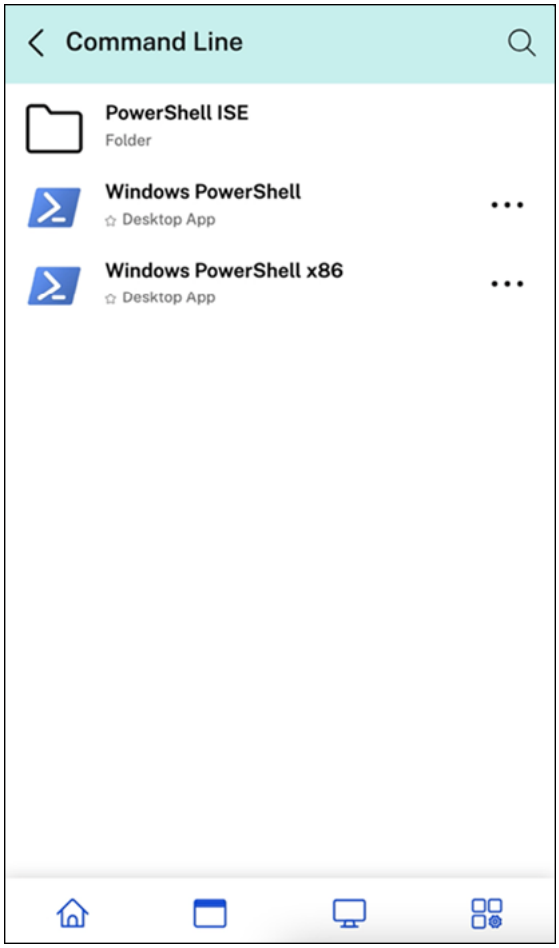
- The Activity Manager panel displays active sessions across all the stores that the user is currently signed into.
- Activity Manager operations such as Logout, Disconnect, and more are not supported for applications that have policies enabled.

23.36

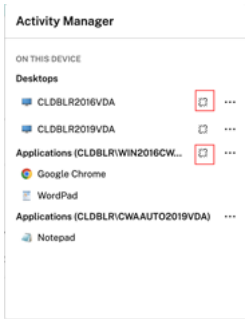
View sub-categories for applications on mobile platforms End users can now view their apps organized into categories and sub-categories on android and iOS devices, providing easy access and a pleasant app browsing experience. To view categories, navigate to the Apps tab and click the Categories dropdown.



Select the relevant category, a list of available sub-categories and applications is displayed based on the configuration made by the admin. Sub-categories are displayed as folders that might contain further sub-folders or applications as per the admin configuration. For more information, see Add folder path

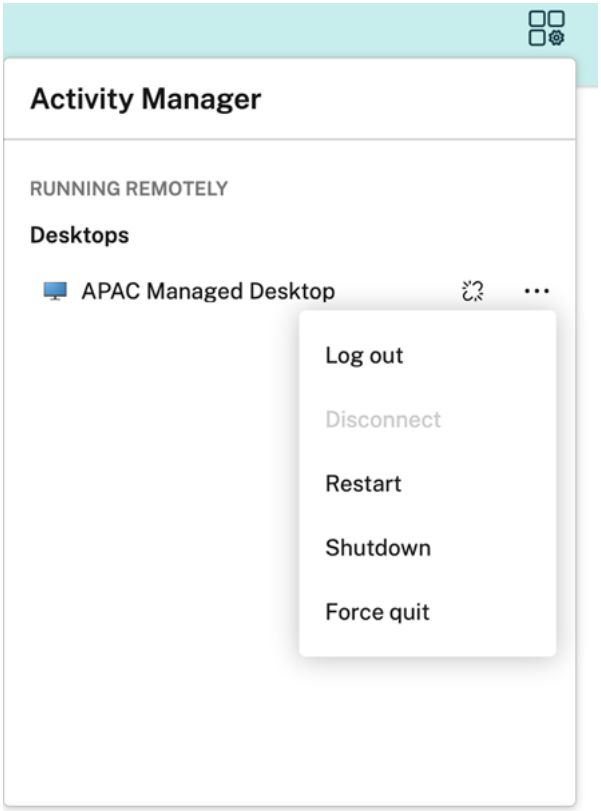


Manage disconnected sessions on Activity Manager from any device Activity Manager now enables end users to view and take actions on apps and desktops that are running in disconnected mode, locally or remotely. Sessions can be managed from mobile or desktop devices, enabling end users to take action on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

For more information, see Disconnected apps and desktops in Activity Manager.

Fixed issues This release addresses areas that improve overall performance and stability.

23.35

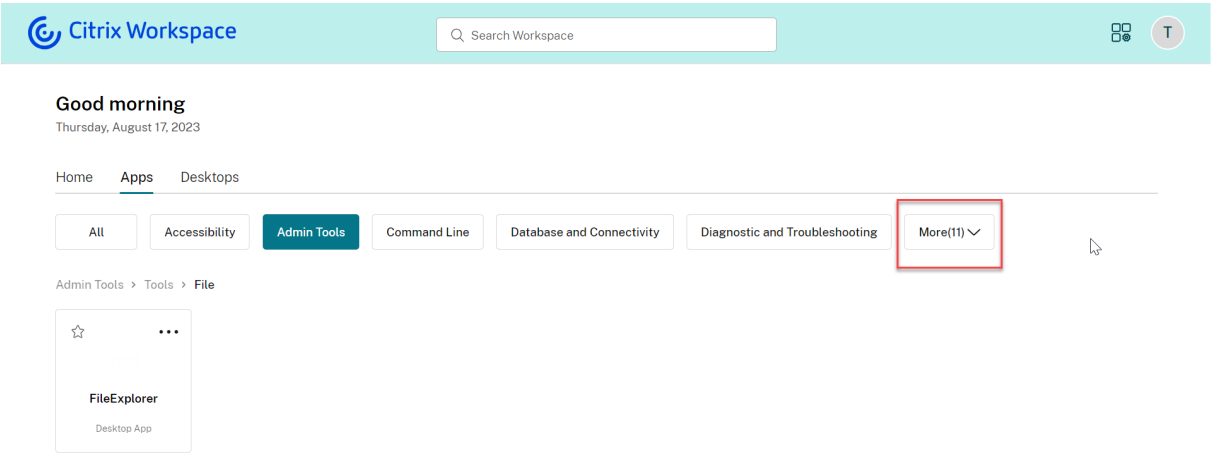
This release addresses areas that improve overall performance, stability, and feature enhancements.

23.34

This release addresses areas that improve overall performance, stability, and feature enhancements.

23.33

Enhanced user experience with 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.

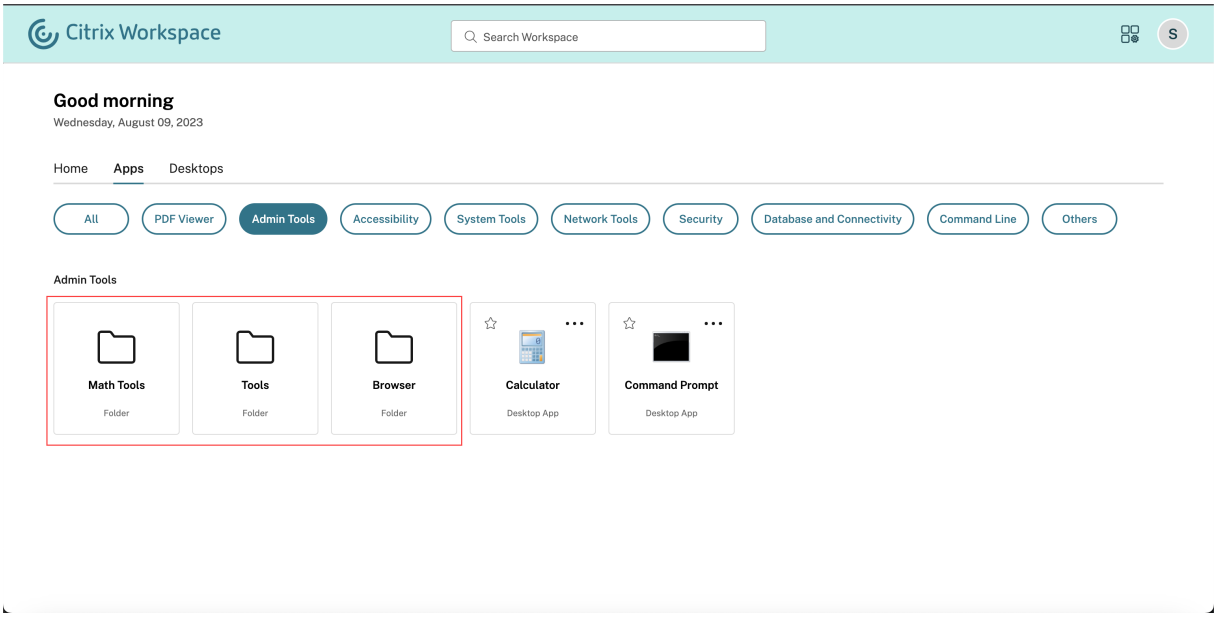


Fixed issues This release addresses areas that improve overall performance and stability.

23.32

App categorization for easy access Admins can deliver apps organized into categories and subcategories, providing a pleasant app browsing experience for their end users. 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.



Fixed issues This release addresses areas that improve overall performance and stability.

23.31

This release addresses areas that improve overall performance, stability, and feature enhancements.

23.30

Manage Activity Manager As an admin, you can now enable or disable the Activity Manager feature for your end users. As per your organization policies, you can enable the feature for everyone or selected users and user groups. When enabled, the Activity Manager panel lets your end users view and interact with their active apps and desktops. For more information, see Activity Manager.

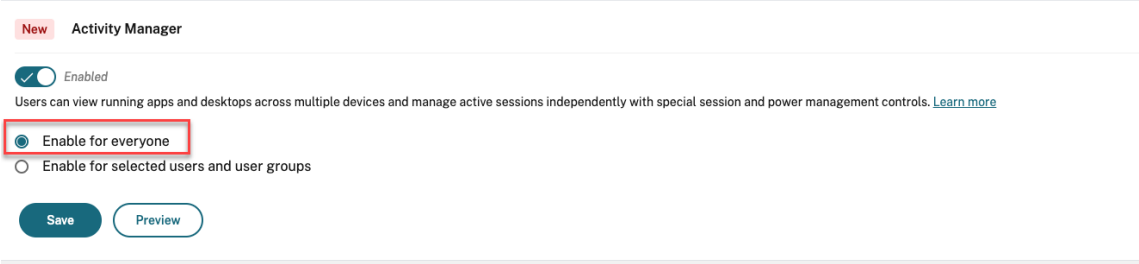
> **Note:**
>
> This feature is supported only for virtual apps and desktops. It is not applicable to web and SaaS apps.

To enable Activity Manager:

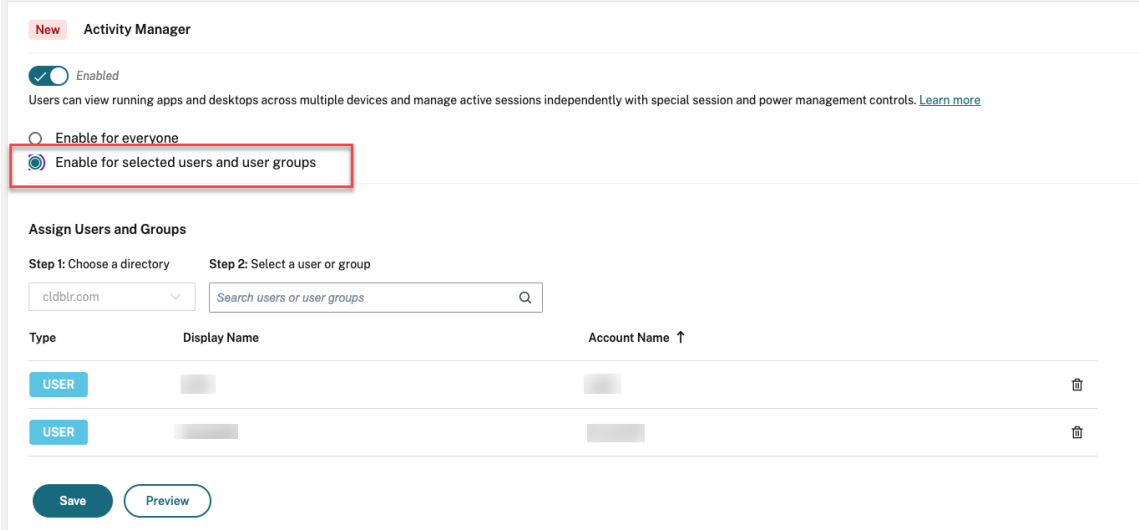
1. On the Admin console, go to **Workspace Configuration** > **Customize** > **Features**.
2. In the Activity Manager section, turn-on the toggle to enable Activity Manager.

3. You can then customize the access permissions as follows.

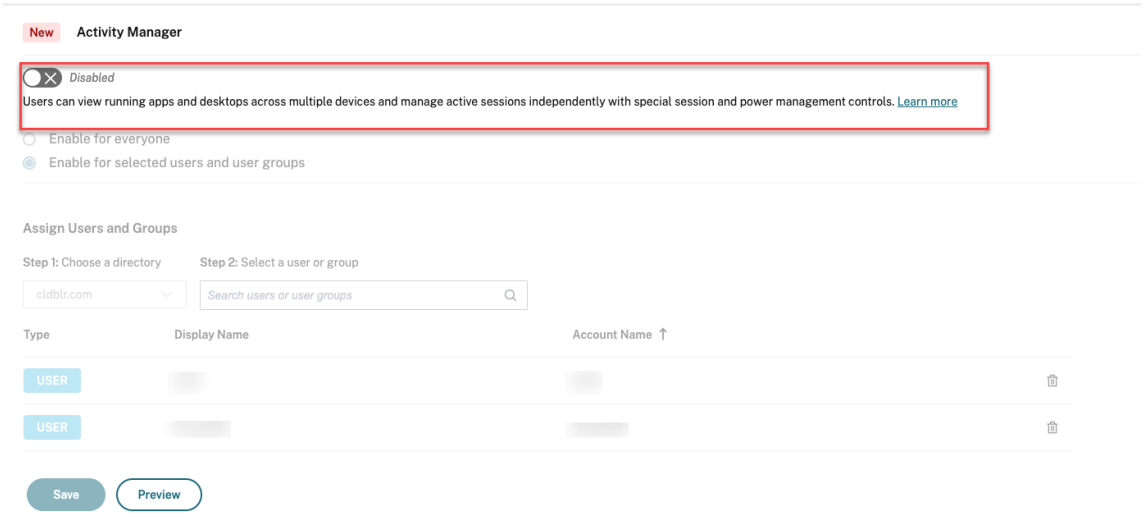
   - To enable Activity Manager for all end users, select **Enable for Everyone**.



   - To enable Activity Manager for selected users and user groups, select **Enable for selected user and user groups**. You can then select the directory to which the users or user groups belong. Once the appropriate directory is selected, you can view relevant users and user groups.



   - To disable Activity Manager for everyone, turn-off the toggle.



4. Click **Save**.

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

23.29

This release addresses areas that improve overall performance, stability, and feature enhancements.

23.28

Deprecation announcement for Internet Explorer UI version 23.26 is available on Internet Explorer till the last week of 2023. Citrix does not support new features, bug fixes, or security patches post the 23.26 release. Additionally, administrators receive a notification to upgrade to the supported browsers and supported LTSR (LTSR2203 or later).

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

23.27

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

Fixed issues

- With this fix, error boundary and component level error handling have been implemented. [WSUI-7423]

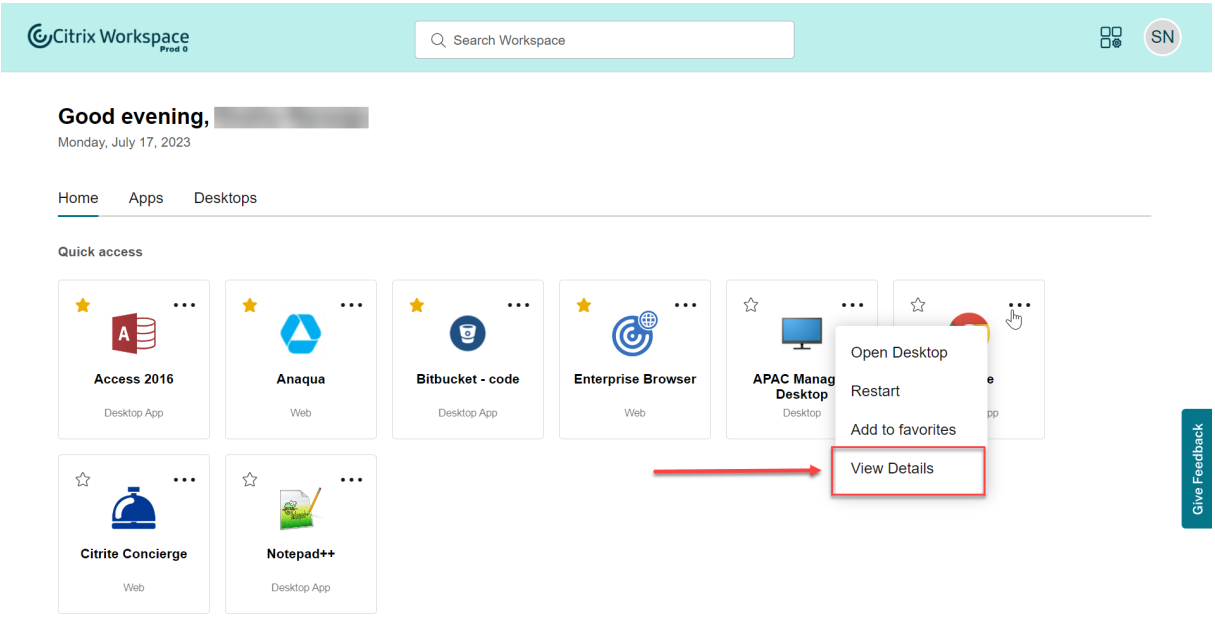
- Offline banner gets minimized once you click the ellipses icon. [WSUI-7797]

23.26

This release addresses areas that improve overall performance, stability, and feature enhancements.

23.25

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**.



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

23.24

This release addresses areas that improve overall performance, stability, and feature enhancements.

23.23

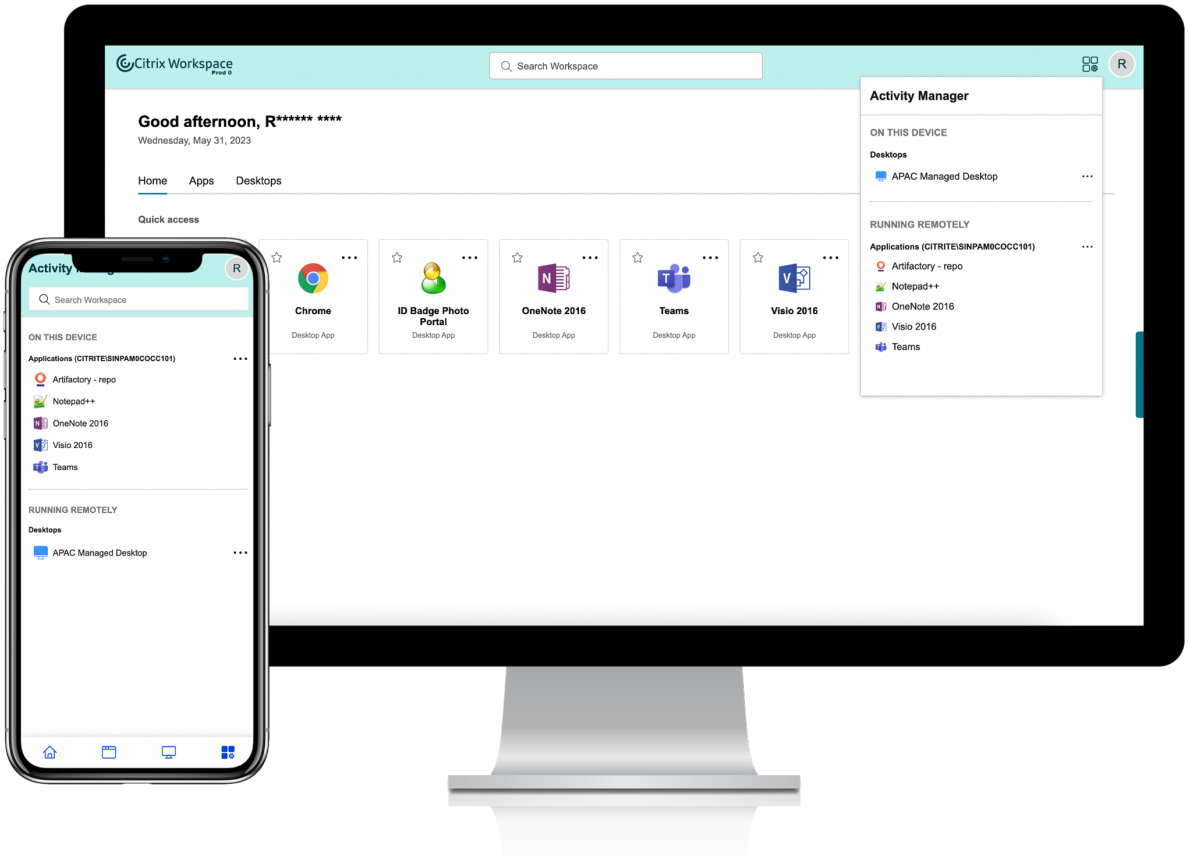
This release addresses areas that improve overall performance, stability, and feature enhancements.

23.22

Introducing Activity Manager You can now manage and take quick actions on the apps and desktops that are active across any device from a single window pane within the Workspace UI. All the active apps and desktops are grouped in the session that you're currently using.

The Activity Manager icon appears on the Workspace UI window to the left of the profile icon. When you click the icon, you see the following:

- A list of apps and desktops started from the device that you're using under **On this device**.
- A list of apps and desktops active on other devices under **Running Remotely**.



For more information, see Activity Manager.

> **Note:**
>
> If you are unable to view the Activity Manager icon clearly, consider changing 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.

Known issues

- If a session gets disconnected, users will not be able to log out from it. Disconnected sessions are not displayed on the Activity Manager panel.
- On , the list of active apps and desktops displayed on the Activity Manager panel lists active sessions from all the stores.

23.15

New Workspace user interface introduces new UI capabilities with a modern look and feel for a cleaner view. The UI enhancements are applicable for web, desktops, and mobile.

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.

Admin related tasks

As an admin you can customize the user experience of the Workspace app for your subscribers. See the following sections for more information

- Enable the new Workspace experience for users
- Enable or disable Home screen for users

What's new in Global App Configuration service

April 11, 2024

The following sections list the new features in current and earlier releases for the Global App Configuration service.

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:

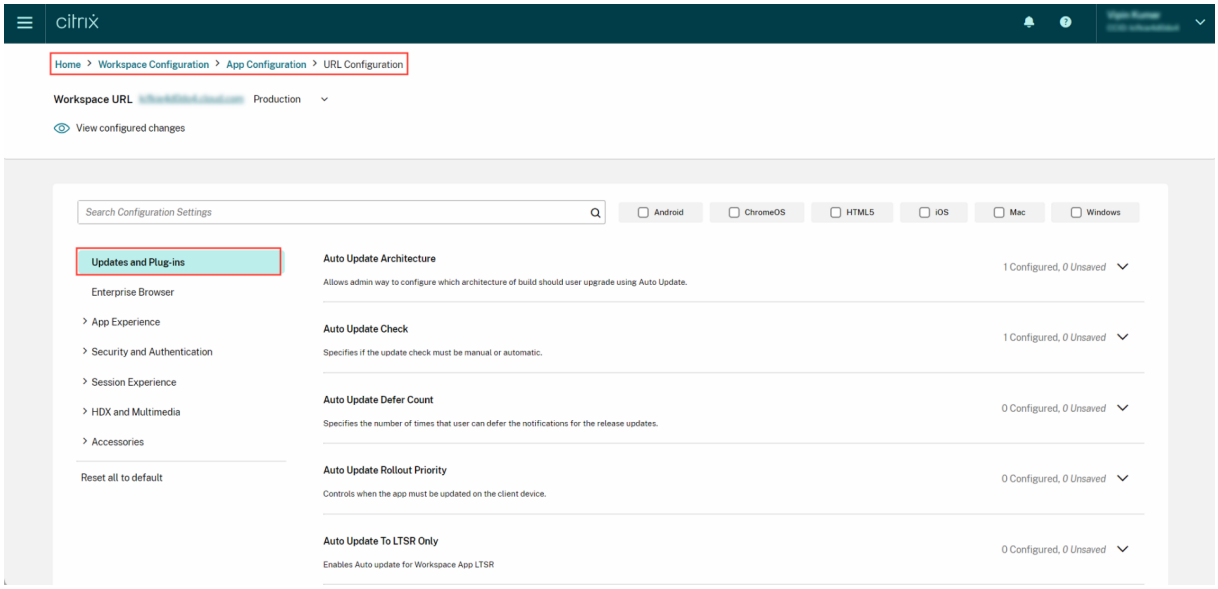
- Autofill suggestions for the addresses
- Autofill suggestions for credit card information
- Launch an external application without prompting the user
- Display the security warnings when potentially dangerous command-line flags are used to launch the browser.
- Manage the default cookie setting
- Manage 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:

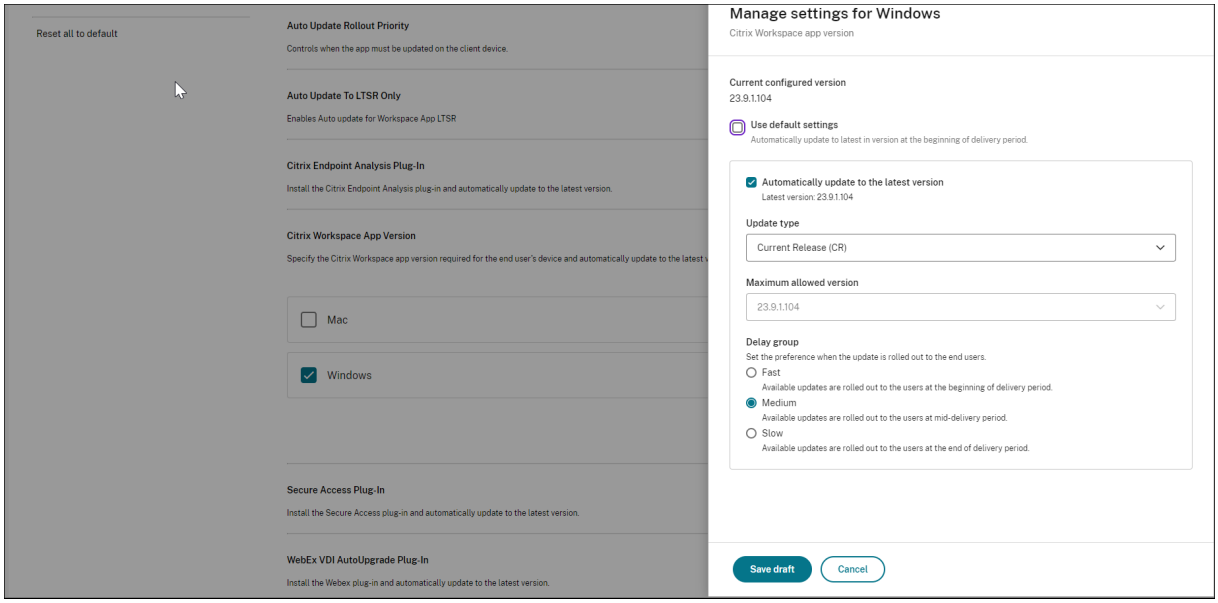
- Citrix Endpoint Analysis Plug-in
- Citrix Secure Access Agent
- Webex VDI AutoUpgrade Plug-in
- Zoom VDI Plug-in Management

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.



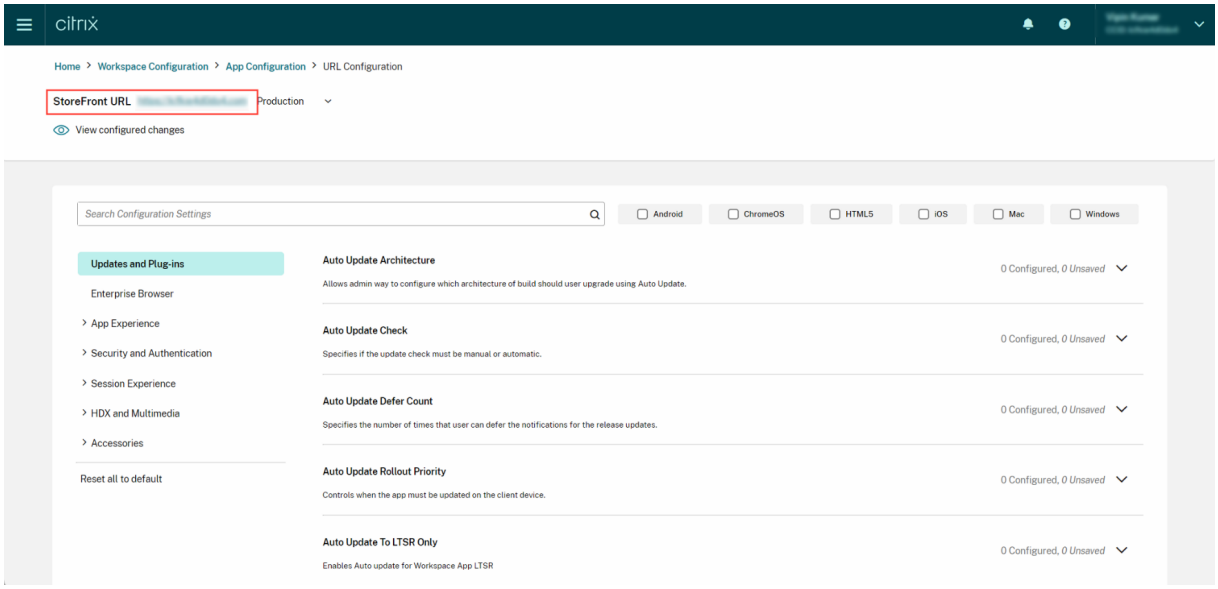
Oct 30, 2023

Configure settings for on-premises stores

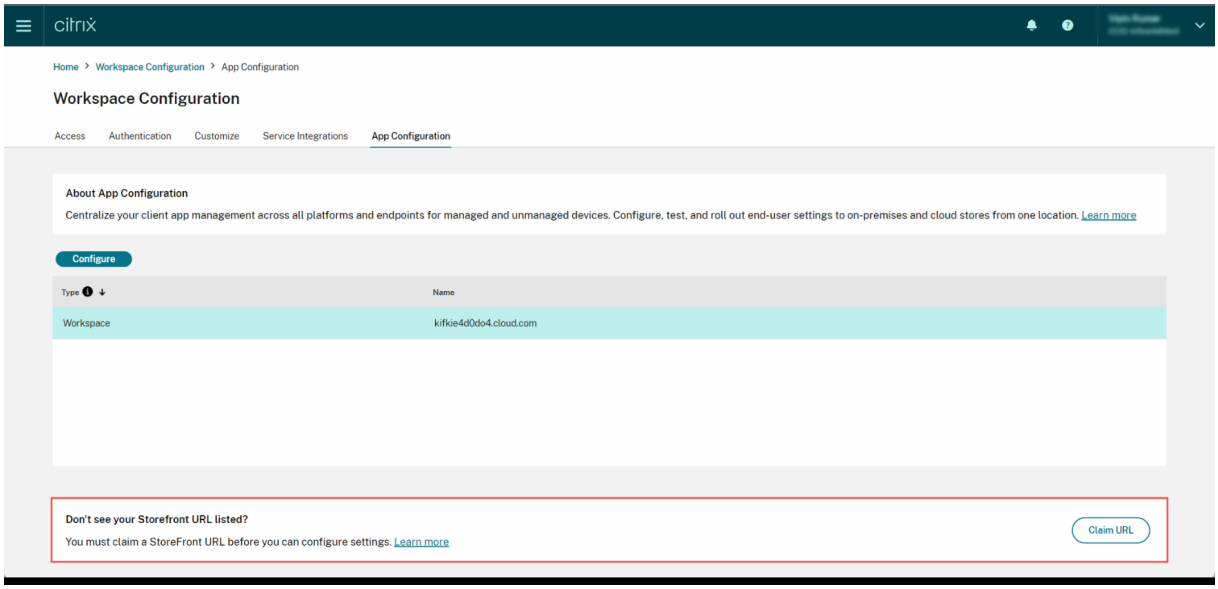
You can now use the Global App Configuration service UI to configure settings for on-premises stores. Sign in to your Citrix Cloud account and navigate to **Workspace Configuration > App Configuration** to get started.

> **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.



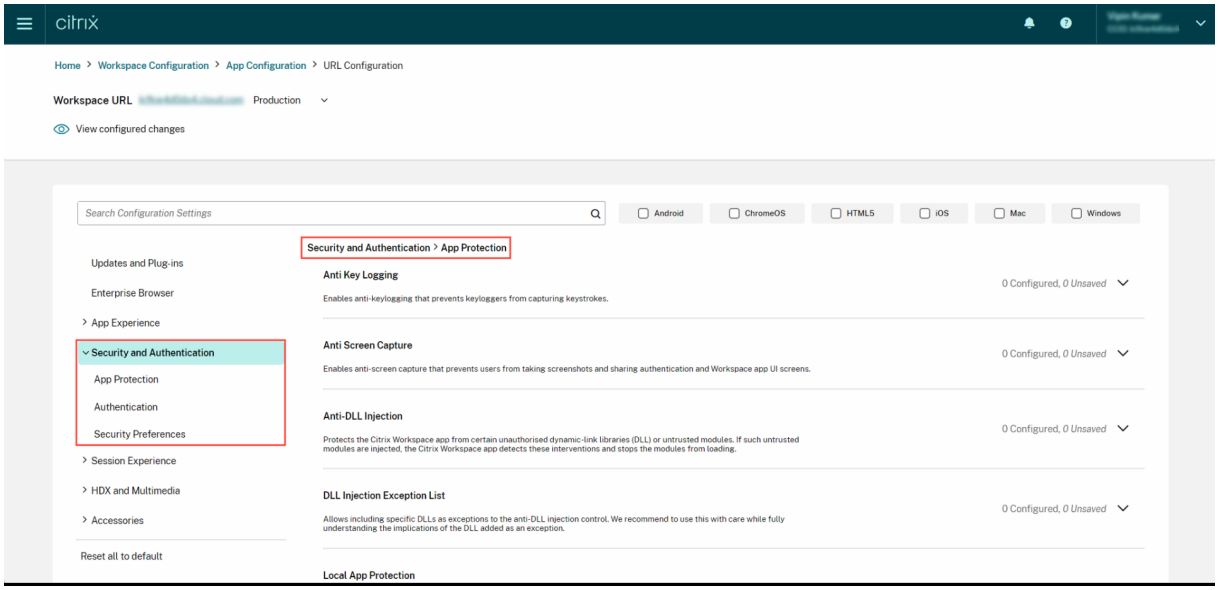
If you haven't claimed your StoreFront URL yet, you can claim it. For that, click **Claim URL** under the **App Configuration** section to claim your URL. For more information, see Get started with configuration.



Sep 28, 2023

Simplified settings categorization for easy navigation

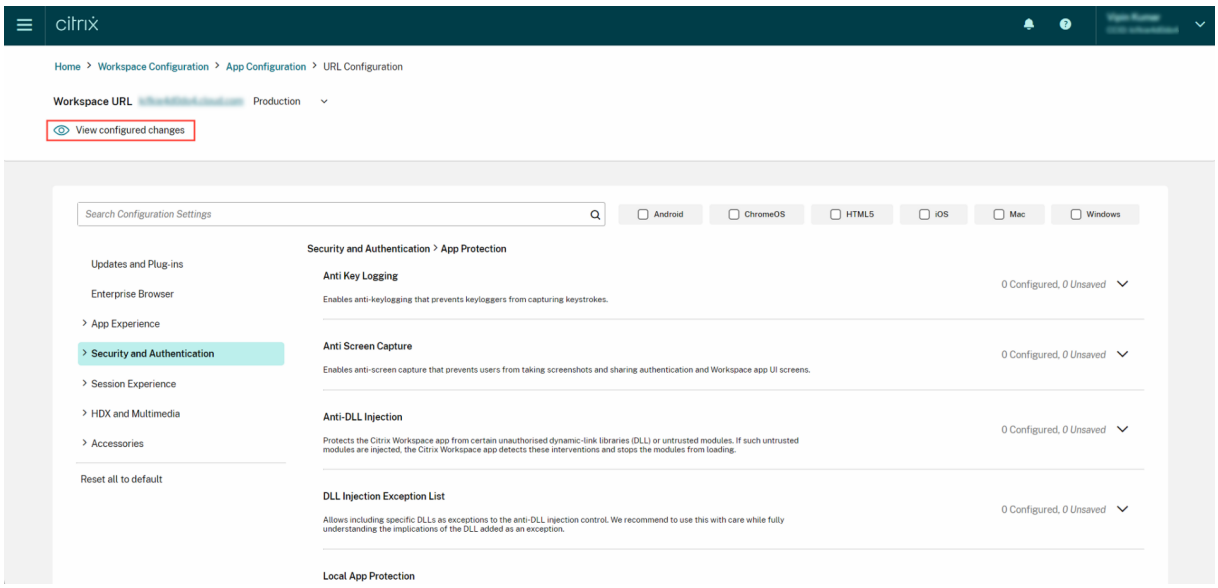
The Global App Configuration service UI has been enhanced to deliver a user-friendly categorization of settings. The settings have been categorized based on end-user workflows and topics, comprising seven primary folders and multiple subfolders. This clutter-free organization makes it easier for admins to navigate among 300+ settings.



Jul 28, 2023

View summary of configured settings

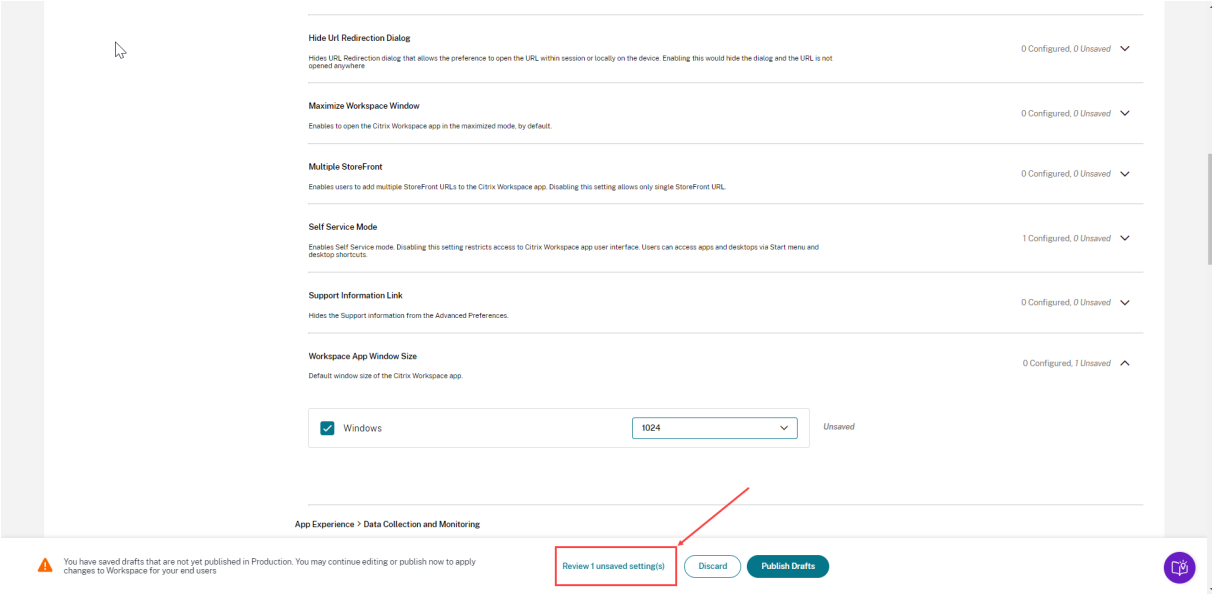
Admins can now view a summary of the current configuration by clicking the **View configured settings** button. This eliminates the need to expand and review each setting separately. A consolidated list of all the configured settings allows admins to perform a comprehensive review of the current configuration and gauge the user impact.



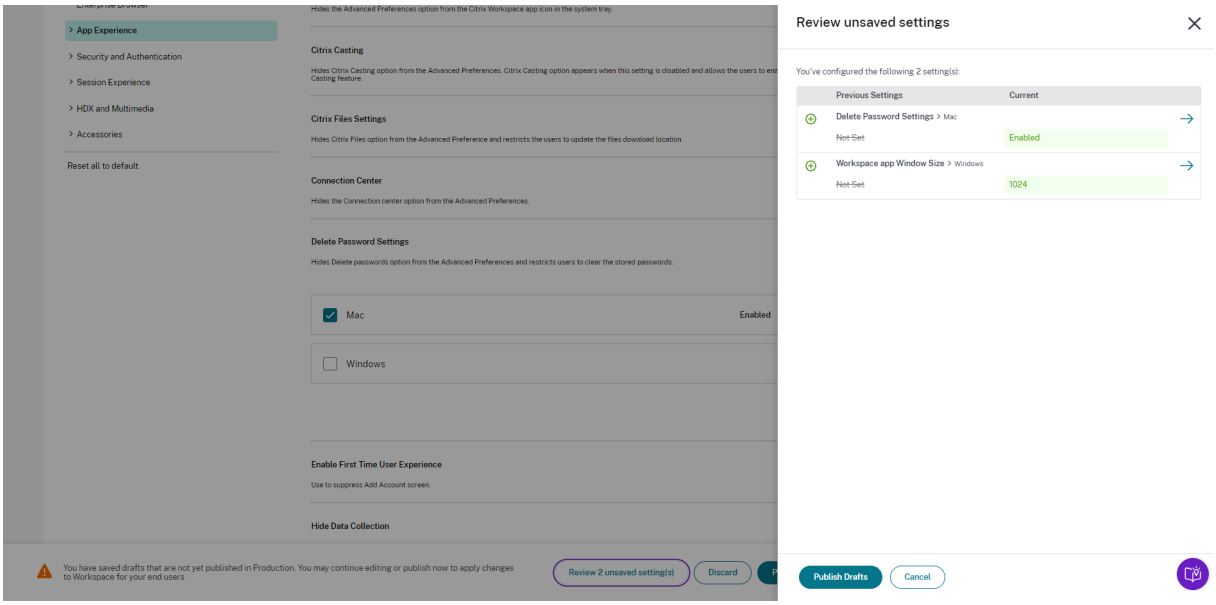
Jun 07, 2023

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.



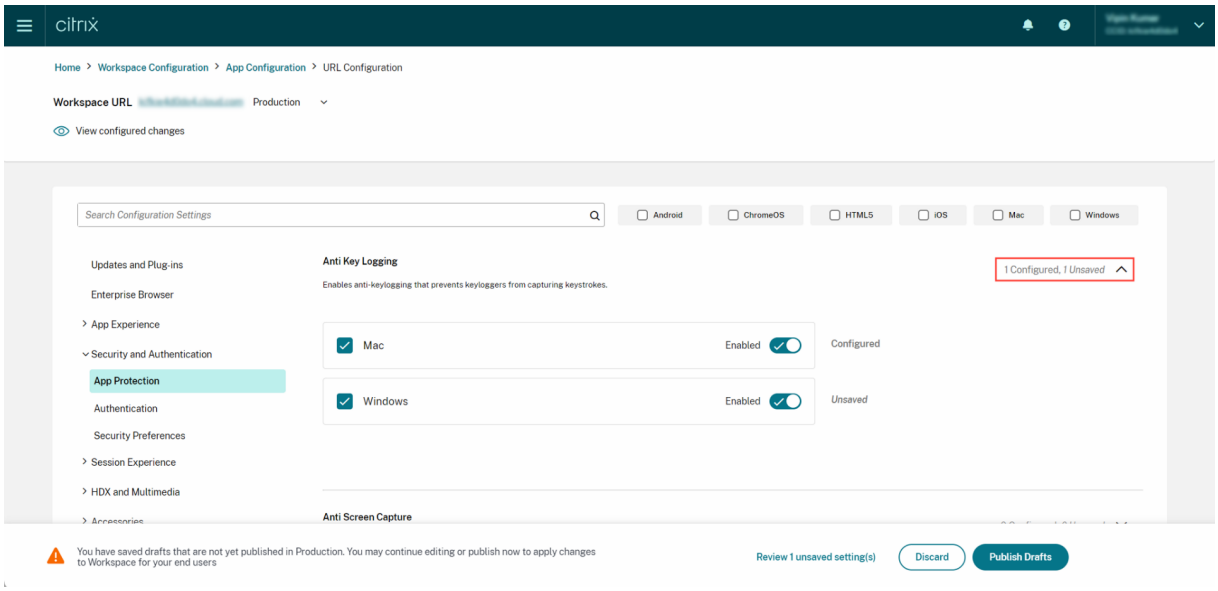
Admins can also navigate to an unsaved setting by clicking the arrow.



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

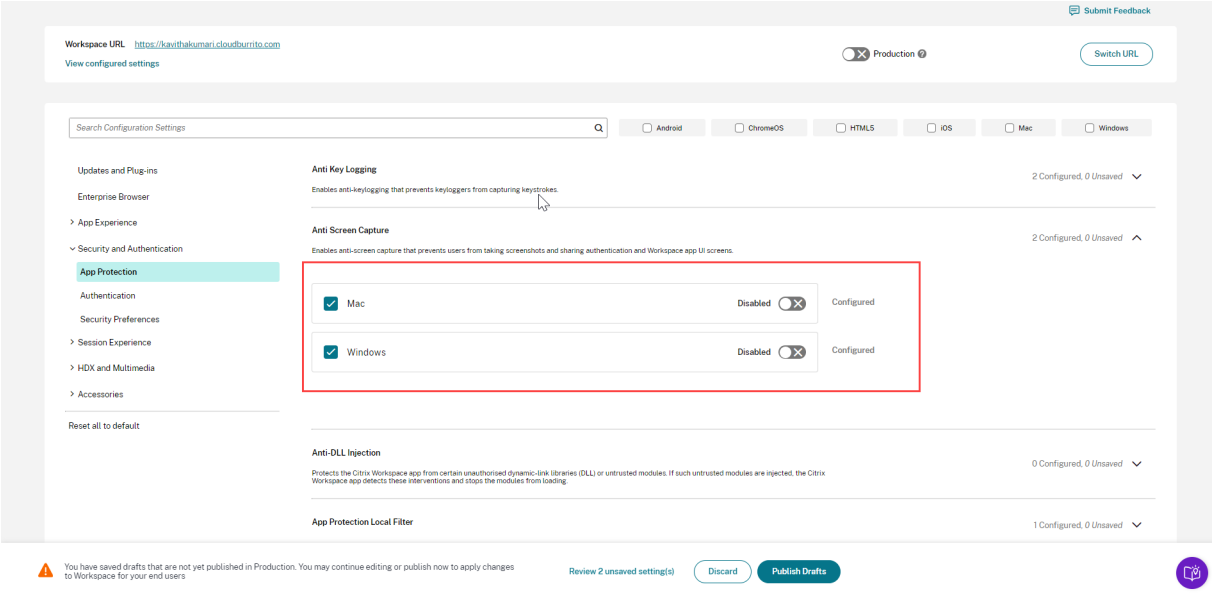
Enhanced search capabilities

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.



Get started with Citrix Workspace

November 17, 2023

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

There are other ways to transition to the full Citrix Workspace experience. The most common are by:

- Delivering Citrix Virtual Apps and Desktops through workspaces.
  - If you want to access resources in your on-premises Virtual Apps and Desktops deployment through Workspace, see Site aggregation for hybrid solutions.
  - If you want to migrate to the cloud, see Full migration to the cloud.

Workflow overview

If setting up Citrix Workspace as a new customer, there are 5 broad phases of work:

1. Prepare for Citrix Workspace in Citrix Cloud.

2. Configure subscriber access and authentication.
3. Integrate services into workspaces.
4. Customize workspaces with your enterprise-specific preferences, such as logos and security policies.
5. Roll out Citrix Workspace to subscribers.

The Success Center provides additional solution-based guidance.

Phase 1: Prepare for Citrix Workspace in Citrix Cloud

Before configuring Citrix Workspace, you must sign up to Citrix Cloud and ensure that you meet the technical requirements for getting started with Citrix Workspace.

If you're already a Citrix Cloud customer, with administrators added through **Identity and Access Management**, you can skip to Phase 2: Configure subscriber access and authentication.

The steps involved in Phase 1 include:

1. Signing up to Citrix Cloud.
2. Adding administrators with a Citrix Identity.
3. Setting up the infrastructure by:
    - Creating resource locations
    - Deploying cloud connectors

Configuring Citrix Identity involves a time-based one-time password (TOTP). In addition to Citrix Identity, you can configure Azure AD authentication. For more information on adding administrators and configuring authentication, see Administrators in the Citrix Cloud product documentation.

Phase 2: Configure subscriber access and authentication

Phase 2 involves configuring access controls, such as the Workspace URL and external connectivity, in **Workspace Configuration**.

You also configure one or more identity providers in **Identity and Access Management**, and then enable one of them as the primary way in which subscribers authenticate to workspaces in **Workspace Configuration**.

> **Note:**
>
> There are two ways to access Citrix Workspace. One is through the natively installed Citrix Workspace app, which replaces Citrix Receiver for simple, secure access to Citrix Cloud services and workspaces. The other way to access Citrix Workspace is through a browser with the Workspace URL. The Workspace URL is enabled by default, usually in the format:

> `https://yourcompanyname.cloud.com`.
>
> For more information, visit Workspace access.

Configure workspace access

You configure access controls in **Workspace Configuration > Access**. It typically involves the following tasks:

- Configure and enable the Workspace URL.
- Configure external connectivity with Citrix Gateway.

After these two tasks, Citrix recommends that you install, and encourage subscribers to use, the Citrix Workspace app for a consistent experience of the workspaces.

Configure subscriber authentication to workspaces

Defining how subscribers authenticate to sign in to their workspaces is a two-step process:

1. Under **Identity and Access Management**, configure identity providers.
2. Under **Workspace Configuration > Authentication**, choose one of the authentication methods delivered by the identity providers you configured in the first step.

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

For more information on configuring subscriber authentication to workspaces, visit Secure workspaces.

Phase 3: Integrate services into workspaces

Integrating your services into workspaces is another two-part process:

1. Configure your purchased services in Citrix Cloud. For a list of services, visit Citrix Cloud Services.
2. Enable access to your configured services in **Workspace Configuration > Service Integrations**. For more information on service integration, visit Enable and disable services.

Phase 4: Customize workspaces

You can customize the subscriber experience of workspaces for different users and to meet specific organizational requirements in **Workspace Configuration** by:

- Customizing the appearance of workspaces, including logos and custom themes. For instructions on customizing Workspace appearance, visit Customize the appearance of workspaces.
- Choosing interaction options, such as allowing subscribers to create **Favorites** and automatically launching desktops. For instructions on customizing how subscribers interact with their workspaces, visit Customize workspace interactions.
- Customizing privacy and security settings. This includes setting a timeout period, creating a sign-in policy, and allowing subscribers to change their passwords from within their workspaces. For instructions on how to customize Workspace privacy and security policies, visit Customize security and privacy policies.

Phase 5: Roll out Citrix Workspace to subscribers

Citrix recommends that you verify the integrity of workspaces with operational acceptance testing and engage with our Success Center to plan how you onboard subscribers. The broad activities for this phase include:

1. Testing workspaces.
    - Verify that you can sign in through the browser and into the Citrix Workspace app.
    - Launch and use all available apps and desktops.
    - Check that you can access available folders and files.
    - Check that notifications are displaying the expected actions and activities.
    - If enabled, verify that you can access endpoint resources on mobile devices.
2. Onboarding subscribers.
    - Communicate Citrix Workspace capabilities with subscribers.
    - Share the browser Workspace URL.
    - Guide users to install the Citrix Workspace app.

For more information on testing workspaces and onboarding subscribers to workspaces, visit Citrix Workspace end-user adoption resources.

Prepare for Citrix Workspace

November 21, 2023

This article outlines the requirements and administrative activities to help you prepare for implementing Citrix Workspace. The steps involved in preparing for Citrix Workspace include:

1. Ensure that you meet the System and connectivity requirements for Citrix Cloud.

2. Plan your deployment and rollout of Citrix Workspace.
3. Sign in or sign up to Citrix Cloud.
4. Add administrators to Citrix Cloud and Citrix Workspace.
5. Check your entitlements to cloud-hosted services.
6. Set up the infrastructure needed for Citrix Workspace.

The Success Center is an essential partner to this documentation. Success Center articles offer both a broad solution-based perspective and service-specific details.

The Citrix Cloud documentation offers detailed information on the tasks that are involved in preparing for Citrix Workspace in Citrix Cloud. You can also find the pre-requisites in the same documentation.

System and connectivity requirements

Citrix Cloud is the console through which you view and manage your service entitlements and access **Workspace Configuration**.

If you're already set up for Citrix Cloud, you can skip to the steps outlined in Plan your deployment and rollout.

In sum, Citrix Cloud requires the following configuration:

- An Active Directory domain to manage subscriber authentication to workspaces.
- At least two Citrix Cloud Connectors per resource location.
- A dedicated machine for each Cloud Connector.
- Physical or virtual machines joined to your domain for hosting workloads and other components.

You need at least two physical or virtual machines. You can't install other components on a machine that hosts a Citrix Cloud Connector.

For information on Cloud Connector requirements, see Citrix Cloud Connector Technical Details. For information on installing Cloud Connectors, see Cloud Connector Installation.

Also, the following addresses must be contactable to operate Citrix Workspace:

- `https://*.cloud.com`
- `https://*.citrixdata.com`

For a complete list of required contactable addresses for Citrix Cloud services, see Service connectivity requirements.

Plan your deployment and rollout

Citrix recommends that you prepare a Citrix Workspace support and management plan. Use the Success Center Plan to establish goals, define use cases, identify risks, and create an implementation strategy, which includes the following:

- Establish business outcomes, services you want to add, and user group requirements.
- Identify technical requirements to Set up the infrastructure for Citrix Workspace.
- Build your Workspace team. Assign tasks to delivery teams and Add administrators for your Citrix Cloud account with access to **Workspace Configuration**.
- Plan engagement with process owners and subscribers.
  - Prepare a change strategy and communication plan.
  - Develop training and reinforcement approaches.
  - Conduct impact and stakeholder analyses.

For more information on planning your Workspace deployment and rollout, see the Success Center's Success Readiness Checklist.

Sign in or sign up to Citrix Cloud

If you're signing up as a new customer, follow the instructions found in Signing up for Citrix Cloud.

If an administrator account was already created for your organization, the primary administrator needs to add you to the company account. See Add administrators for more information.

If you already have an account, sign in to Citrix Cloud. You can use your citrix.com, My Citrix, or Citrix Cloud credentials.

For more information on signing in or signing up to Citrix Cloud, see the Citrix Cloud Services Kickoff Guide.

Add administrators

The first administrator account is created through the initial Citrix Cloud onboarding process. The initial administrator can then invite other administrators to join Citrix Cloud. These new administrators can use their existing Citrix account credentials or set up a new account.

Invite administrators

Administrators are added to your Citrix Cloud account through **Identity and Access Management** in the menu on the left side of the Citrix Cloud console. Enter the email address of the administrator that you want to add to send them an invitation with sign-in instructions.

When you add administrators to your Citrix Cloud account, you define the administrator permissions that are appropriate for their role in your organization. Administrators with **Full Access** have access to **Workspace Configuration** by default. Administrators with **Custom Access** have access only to the functions and services that you select. You can change the access permissions of the administrators you invite.

For more information on adding (and removing) administrators, see Administrators.

Set up administrator authentication

Citrix Cloud uses the Citrix identity provider by default to manage your Citrix Cloud account. Citrix identity provider authenticates Citrix Cloud administrators only. Subscribers must authenticate with one of the identity providers listed in Secure workspaces.

Each administrator in your Citrix Cloud account must also set up multifactor authentication (MFA).

Registration involves downloading and installing an authentication app that follows the Time-Based One-Time Password (TOTP) standard, such as Citrix SSO. For smooth registration, Citrix recommends downloading and installing Citrix SSO *before* completing the following steps.

1. Sign in to your Citrix Cloud account.
2. Select your name and choose **My profile** from the drop-down menu.
3. Select **Set up authenticator apps** under **Login security** to receive an email with the verification code needed for step 4.
4. When prompted, enter the verification code sent to you in an email from Citrix and your account password, and then **Verify**.
5. Scan the QR code or enter the key into an authentication app that follows the Time-Based One-Time Password (TOTP) standard, such as Citrix SSO.
6. To confirm that MFA has been set up correctly, enter the 6-digit code from the authentication app and then select **Verify**.
7. Select **Add a recovery phone** and enter a phone number that Citrix Support can reach you on to verify your identity for MFA-related queries.
8. Select **Generate back up code** to create a list of one-time use codes that can be used if you lose access to your authenticator app.
9. Select **Download codes** and keep the text file with your back-up codes in a safe and accessible location.
10. Select the checkbox and then **Finish**.

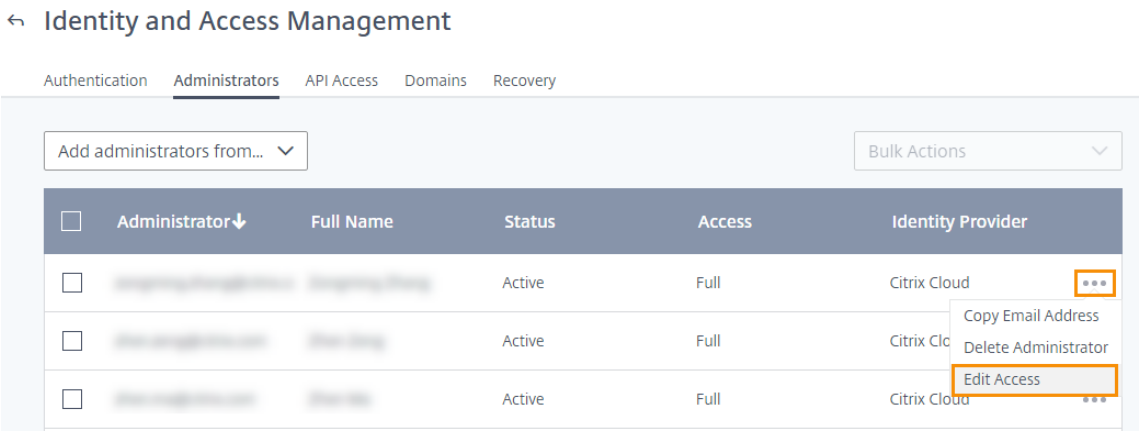
Instructions for setting up MFA can also be found at Knowledge Center, and in Set-up multifactor authentication documents.

You can also optionally set up Azure Active Directory (AD) for administrators. For more information on the identity providers, visit Identity providers.

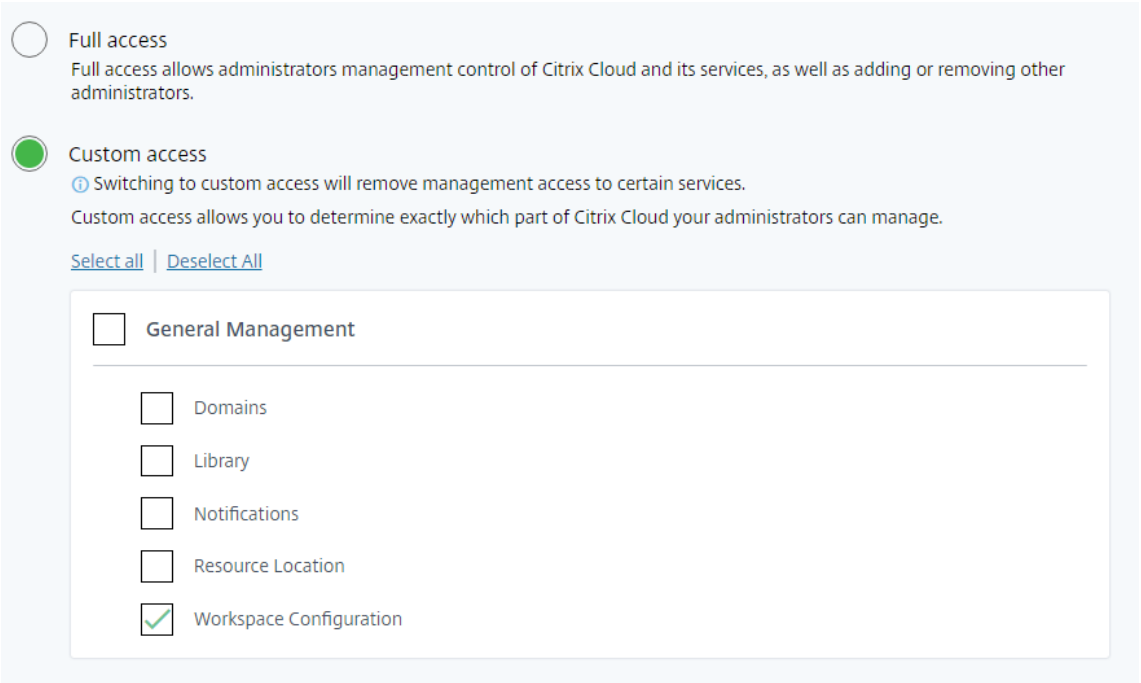
Edit administrator permissions

To configure custom access to **Workspace Configuration**:

1. From the **Citrix Cloud** menu, select **Identity and Access Management** and then select **Administrators**.
2. Locate the administrator that you want to manage, select the ellipsis button, and then select **Edit Access**.

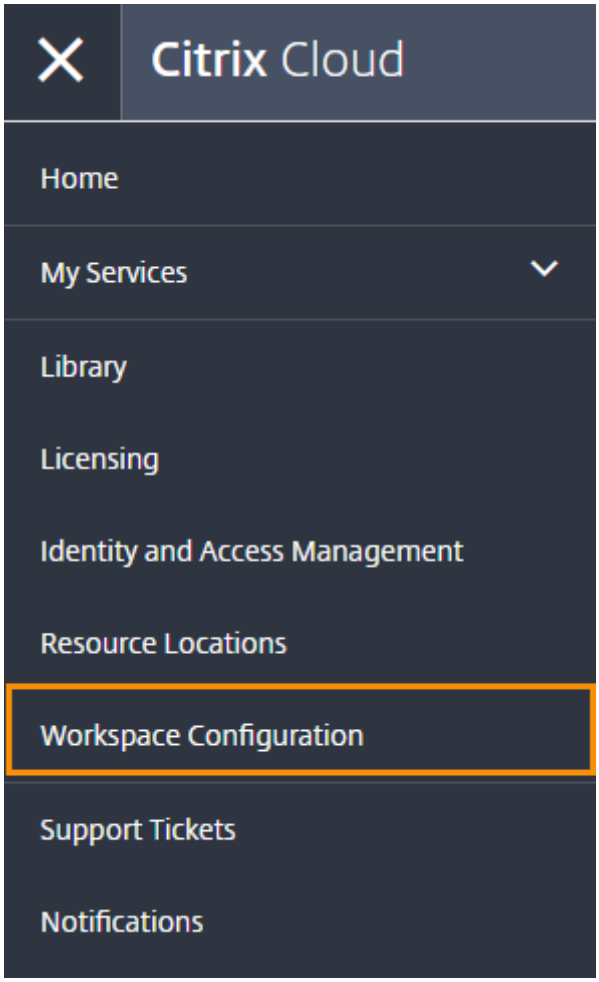


3. Check that **Custom Access** is enabled.
4. To enable only **Workspace Configuration** access, select **Workspace Configuration** under **General Management**.



After enabling access, administrators can sign in to Citrix Cloud and select **Workspace Configuration**

from the **Citrix Cloud** menu.



> **Note:**
>
> In Citrix Virtual Apps Essentials, **Workspace Configuration** is available from the Citrix Cloud menu after you create the first catalog.

Check your entitlements

Once you're signed in to Citrix Cloud, you can manage your entitlements –the Citrix products and services that you purchased. Citrix products and services are displayed in a card layout in the Citrix Cloud dashboard. Products and services that you've purchased and subscribed to include a **Manage** button.

If you'd like to try a new service, you can select **Request Trial** or **Request Demo** in the corresponding box in the Citrix Cloud dashboard. For more information on service trials, visit Citrix Cloud Service Trials.

If you'd like to buy a new service, you can convert a trial into a production service without reconfigu-

ration or creating an account. To buy a service, you need your organization ID that is available in the top-right corner of the Citrix Cloud console. Now visit https://www.citrix.com/product/citrix-cloud.

Set up the infrastructure

Setting up the infrastructure needed for Citrix Workspace involves connecting your resources to Citrix Cloud by:

- Deploying connectors in your environment.
- Creating resource locations.

Resource locations contain the resources required to deliver cloud services to your subscribers. You manage these resources from the Citrix Cloud console. Resource locations contain different resources depending on which services you're using.

To create a resource location, you need to install at least two Cloud Connectors in your domain.

Citrix Cloud Connector is a component that provides a channel for communication between Citrix Cloud and your resource locations. The channel establishes connections to the cloud using the standard HTTPS port (443) and the TCP protocol. No incoming connections are accepted.

For more information, visit Citrix Cloud Connector.

> **Note:**
>
> Workspace doesn't support connections from legacy clients that use a PNAgent URL to connect to resources. If your environment includes these legacy clients, you must instead deploy StoreFront on-premises and enable legacy support. To secure these client connections, use Citrix Gateway on-premises instead of the Citrix Gateway service.

Next: Build your workspace

Now that you're prepared for Citrix Workspace, the next steps are as follows:

- Configure access to workspaces, including the Workspace URL and external connectivity.
- Configure workspace authentication, with instructions in Secure workspaces.
- Integrate services into workspaces.
- Customize the experience of workspaces:
  - Customize the appearance of workspaces.
  - Customize workspace interactions.
  - Customize security and privacy policies.

New user interface on cloud

March 8, 2024

The new user interface (UI) on cloud reduces visual complexity, provides easy access to essential features, and refines your Workspace app use and functionality as needed –resulting in a better user experience.

This article highlights some of the main features that the subscribers see when they sign in to their workspaces, and summarizes how to access and interact with their workspaces.

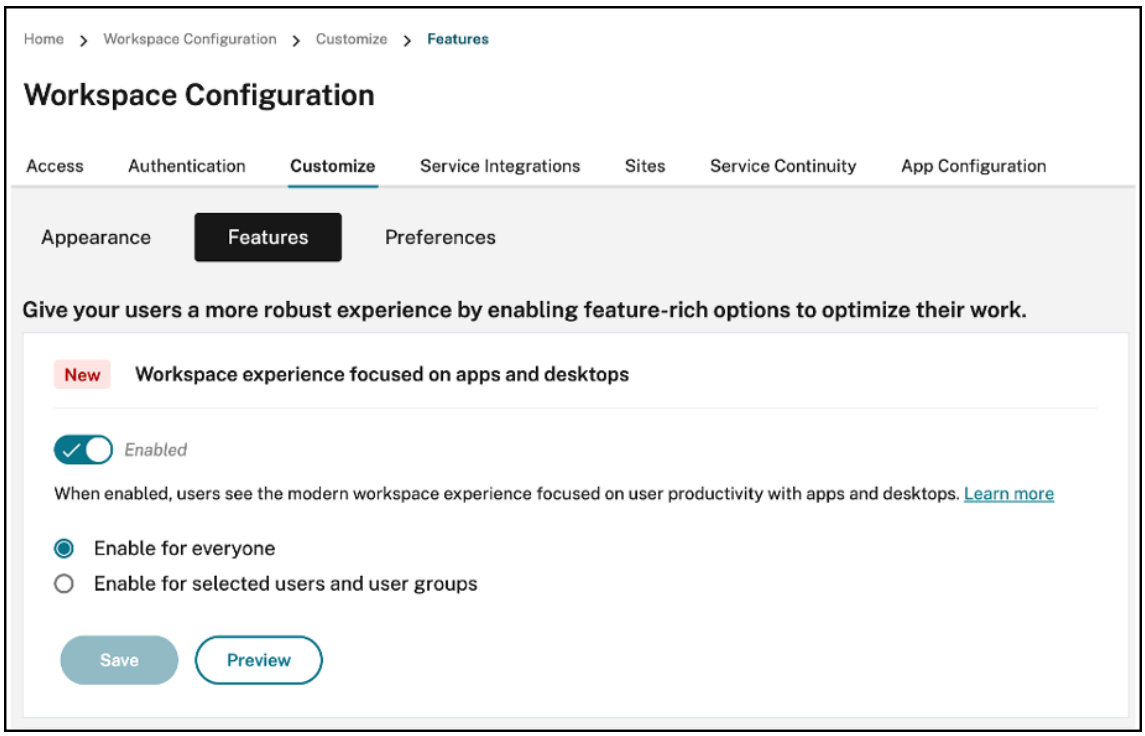
> **Note:**
>
> The new UI is supported with all LTSR versions of Citrix Workspace app. It is also compatible with all web browsers except for Internet Explorer (for which Citrix Workspace UI version 23.26 is frozen).

Enable the new Workspace experience

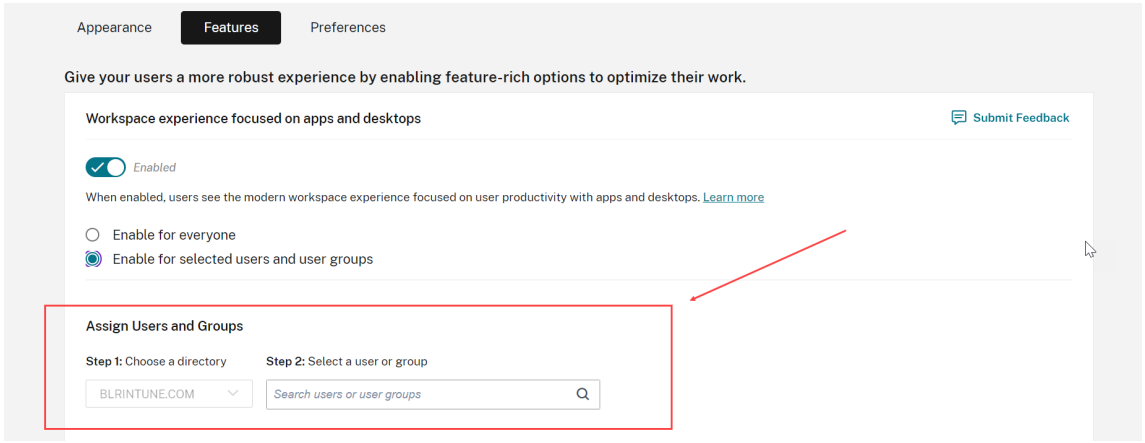
You can enable the new Workspace UI for the existing users. When enabled, users experience the modern workspace focused on productivity with apps and desktops.

To enable the new UI, follow these steps:

1. On the Admin console, go to **Workspace Configuration > Customize > Features**.
2. Turn on the toggle in the **Workspace experience focused on apps and desktops** section. By default the toggle is off, and the feature is disabled.
   You also have the option to enable this feature for all users, or selected users.



- To enable the new UI for all end users, select **Enable for everyone**.
- To enable the new UI for selected users and user groups, select **Enable for selected user and user groups**. You can then select the directory to which the users or user groups belong. Once the appropriate directory is selected, you can view relevant users and user groups.



3. Click **Save**.
4. Restart the Workspace app.

> **Note:**
>
> The updated UI can take around five minutes to display. Users might temporarily see an older

> version of the UI. If opened on a browser, users may need to refresh the page.

Themes, icons, and fonts

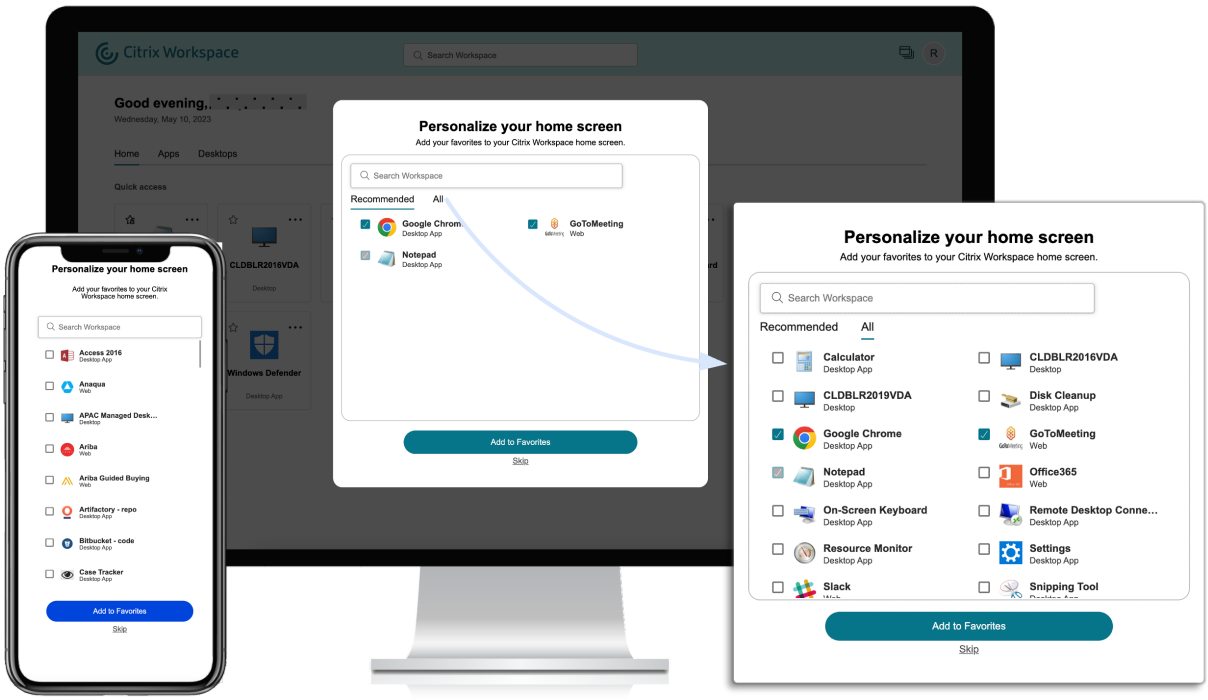
The new color themes have improved contrast and a consistent color palette. The font is used for the UI on all supported operating systems. A new icon set has more distinguishable shapes and colors designed for legibility and visual clarity.

First-time user experience for Workspace app

When accessing the new UI, first-time users are prompted with a pop-up where they can favorite multiple apps in one easy single step.

The first-time user experience is activated when users have more than 20 apps, and haven't added any of them to Favorites. The experience is supported on all browsers and native clients (Mac, Windows, Linux, and ChromeOS), and mobile devices (iOS and Android). You're able to see it the first time you sign in.

The recommended or mandatory apps appear on the **Recommended** tab of the first-time user screen, as set by admins on the DaaS console for Citrix Virtual Apps and Desktops, and on the Secure Private access console for Web and SaaS apps. Mandatory apps are selected by default and check disabled. **Recommended** and auto-favorite apps are selected by default and check enabled for users. End users can also select other apps to subscribe to, or add to Favorites from all tabs. All selected apps are automatically added to Favorites, and reflected on the home page.



When you have five or less apps, on the Citrix Workspace app for Windows, the quick access desktop shortcut appears.
All the displayed apps are subscribed for users, and corresponding desktop shortcuts are created.

Limitations

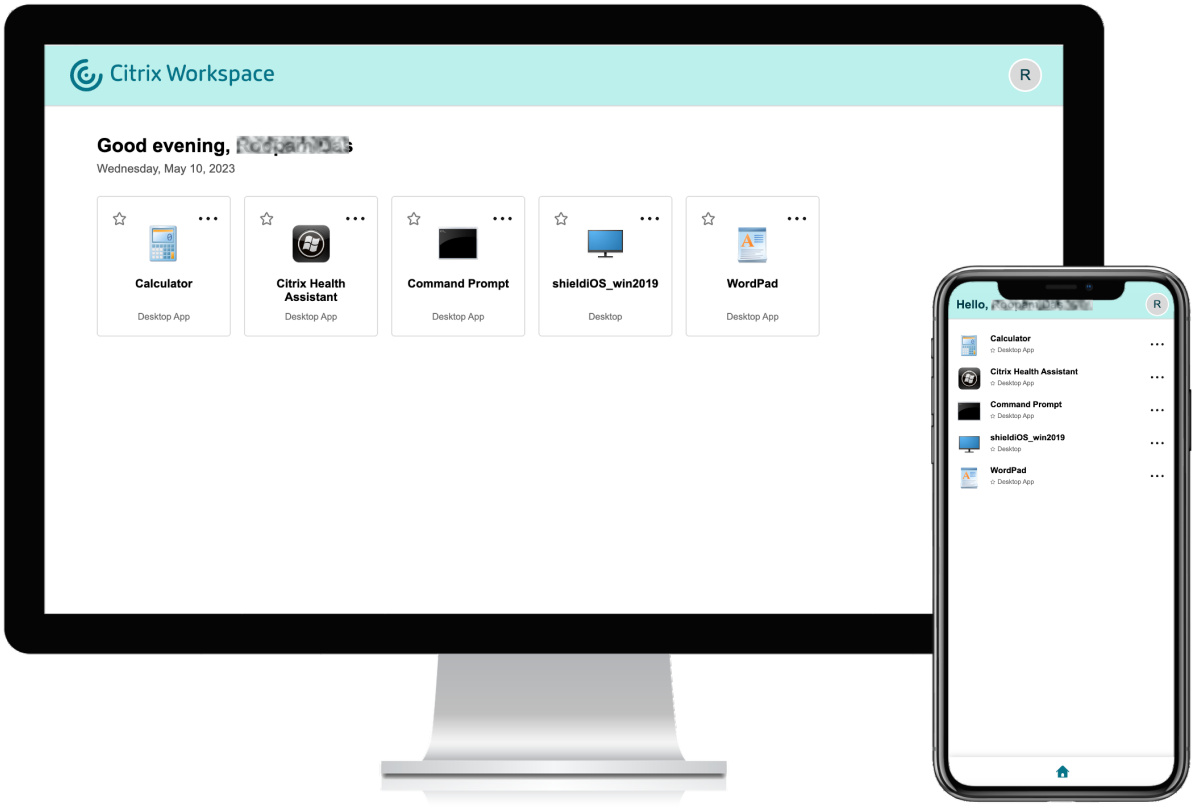
- Until the *User personalization Service* is enhanced to track whether the user is a first-time user or not, the **Personalization** screen appears once per device and browser, and every time for incognito mode unless users mark a favorite.
- If the admin removes the mandatory or recommended tag from the apps, the apps in **Favorites** won't have any impact.
- If the end-user has not added any apps to **Favorites**, the **Personalization** screen appears each time the workspace app is opened.
  To avoid this:
  - End users can add one or more apps to **Favorites**. This prevents the personalization screen from appearing everytime they start the app.
  - Administrators can add one or more apps to Favorites for end-users by using **Description and keyword settings** (keyword: Auto) in Citrix DaaS (**Manage** > **Full Configuration** >

Applications). This prevents the Personalization screen from appearing for all the end-users. For more information, see Customize workspace interactions.

Workspace visual and layout improvements

The new user experience is designed with a focus on intuitive flow and ease of use. Your apps, virtual desktops favorites are organized at the top of the UI for ease of use. Citrix also has a new home page to improve the navigability of your more regularly used apps and desktops.

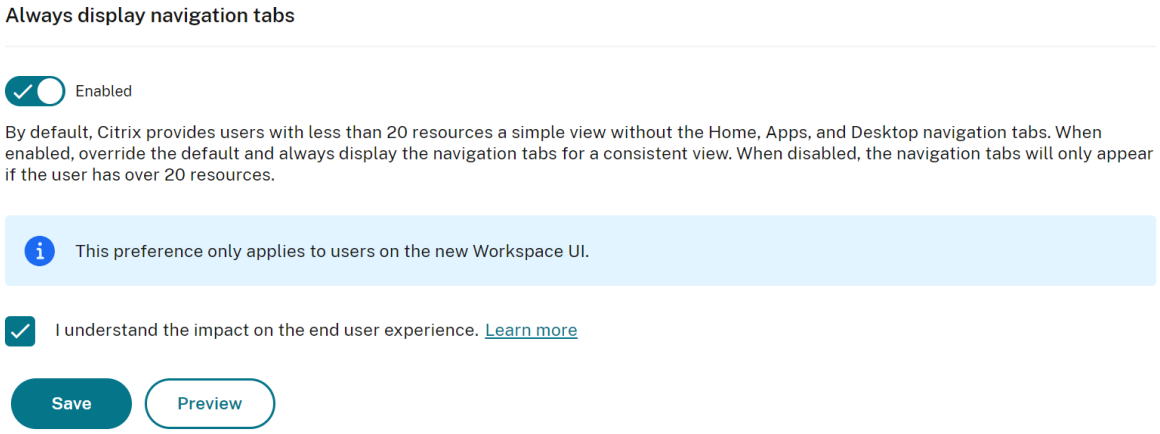
If you have fewer than 20 resources, by default, you land on the screen with Simple View that doesn't have any tabs or categories. All the apps and desktops appear on the same page. On this screen, your favorites show up first, followed by all the other apps in an alphabetical order. All the apps have a star icon that you can use to favorite or unfavorite apps. You experience this Simple View of the Workspace app, depending on the number of apps you have.



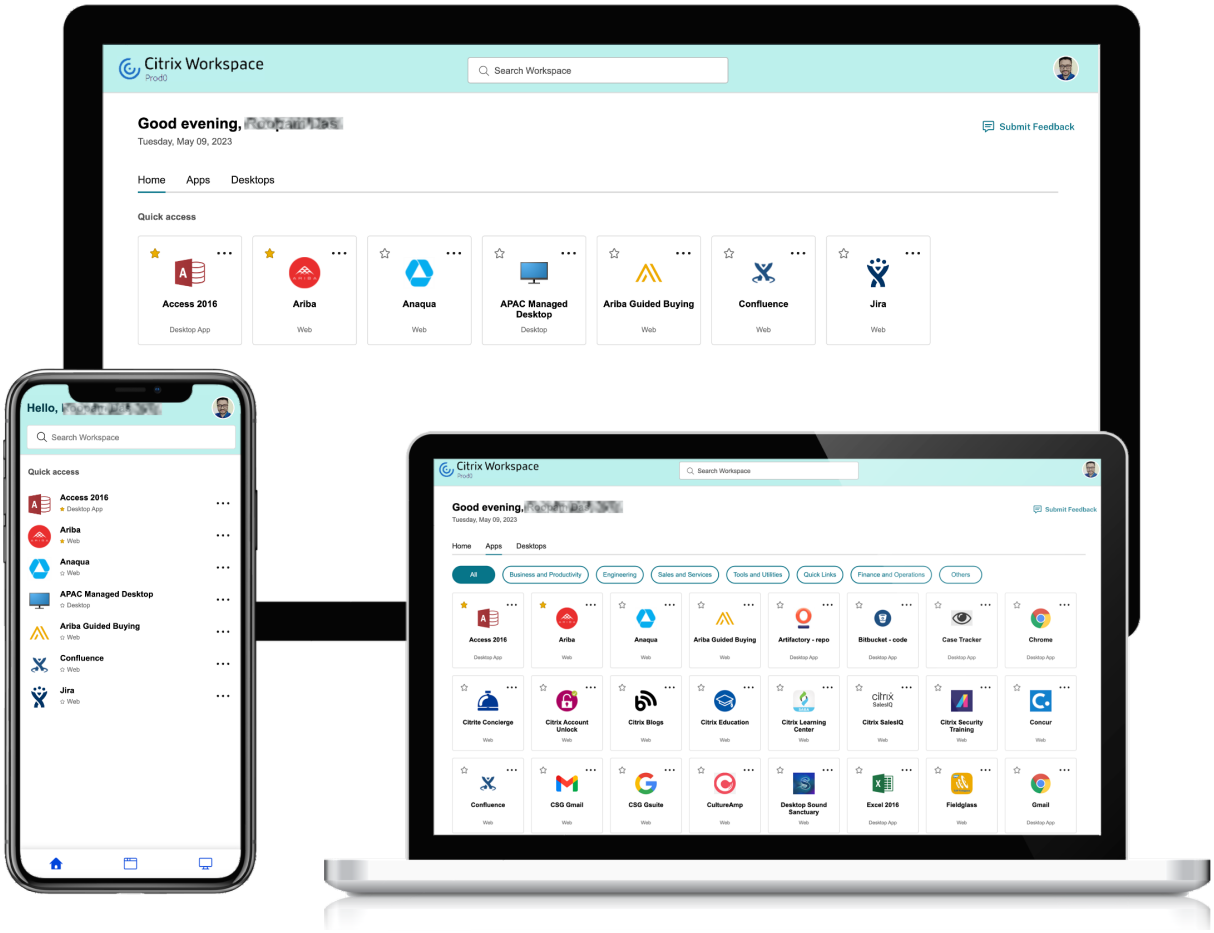
To disable the Simple View and enable the navigation tabs for a consistent experience, even if there are fewer than 20 resources, do the following:

1. Sign in to your Citrix Cloud account and navigate to **Workspace Configuration** > **Customize** > **Preferences**.

2. Enable the toggle button for **Always display navigation tabs**.
3. Select the declaration checkbox, and then click **Save**.



If you have more than 20 resources, you land on the home page when you sign in. On this screen all your favorite apps appear first, followed by the most recently used apps limiting to five apps. The star icons for the **Mandatory** apps are locked, and you can't remove them from Favorites. If the admin hasn't enabled the home page, then you land on the **Apps** screen. On this screen, your favorites appear first, followed by all the other apps in an alphabetical order. If the admin has created categories and attached the apps to them, then the various categories appear, and can select the category of the apps that you want to view.

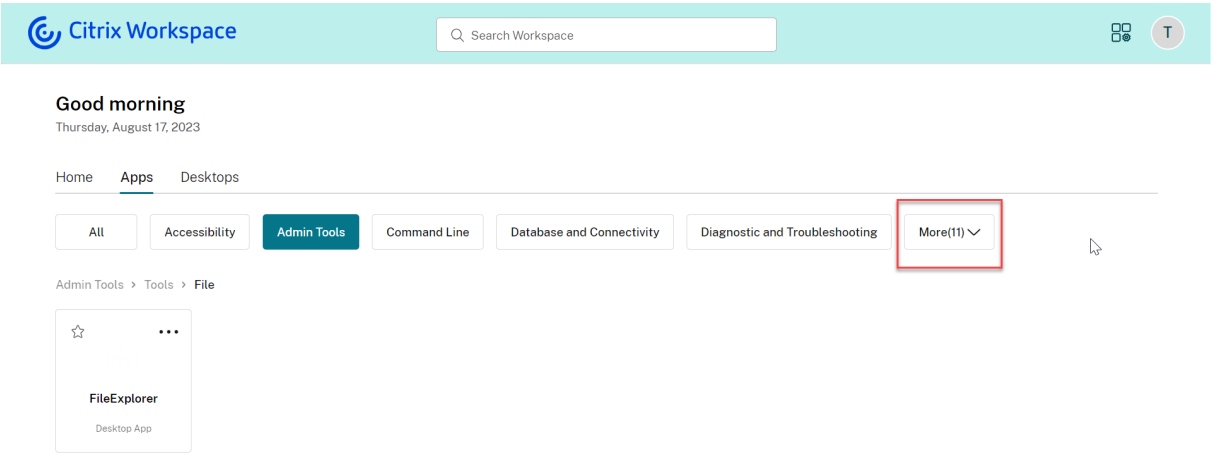


Categorization of apps

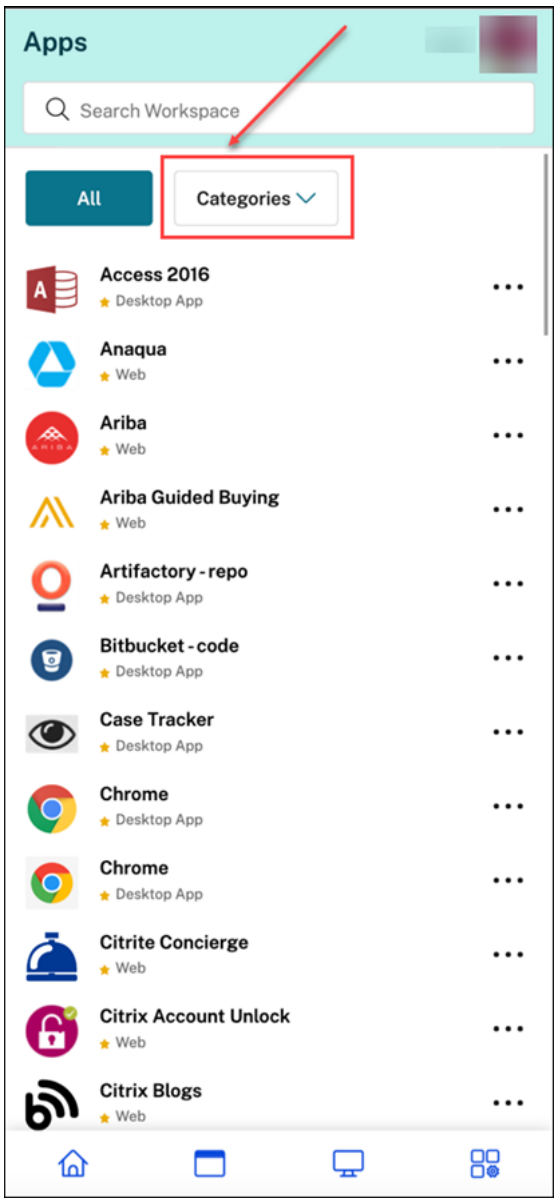
End users can view their applications organized into categories and sub-categories on the Workspace user interface. The sub-categories are displayed in a folder structure. The organized multi-level structure makes for a clutter-free, optimized experience that helps enhance the overall user satisfaction.

> **Note:**
>
> For apps to appear under a folder structure, admins must add a folder path. For more information, see Add folder path.

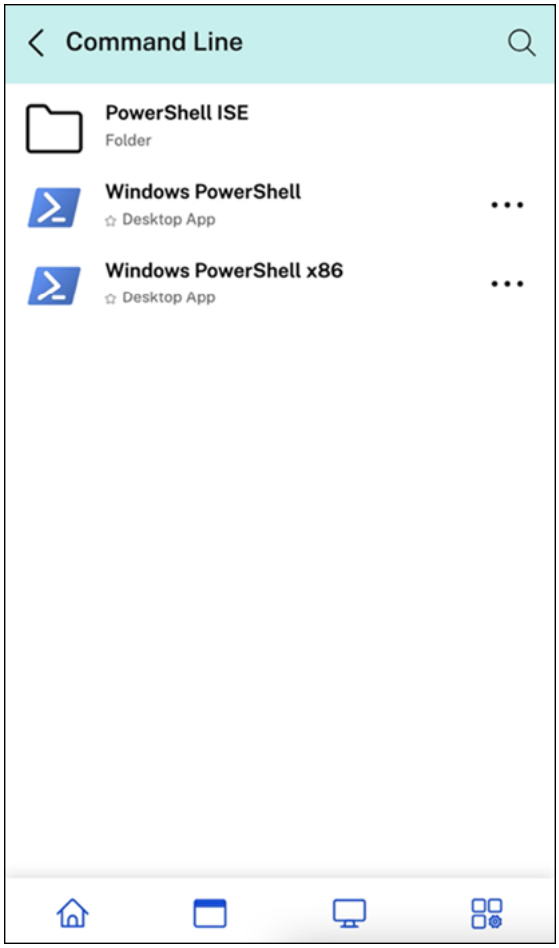
When the number of primary categories created by the admins exceeds the available space on the user's screen, the user interface adjusts based on the screen size, and dynamically moves categories under the **More** dropdown.
The navigation breadcrumbs are also displayed to the users.



On mobile platforms, navigate to the Apps tab and click the **Categories** dropdown to view a list of available categories. Sub-categories are displayed as folders that might contain further sub-folders or applications as per the admin configuration.

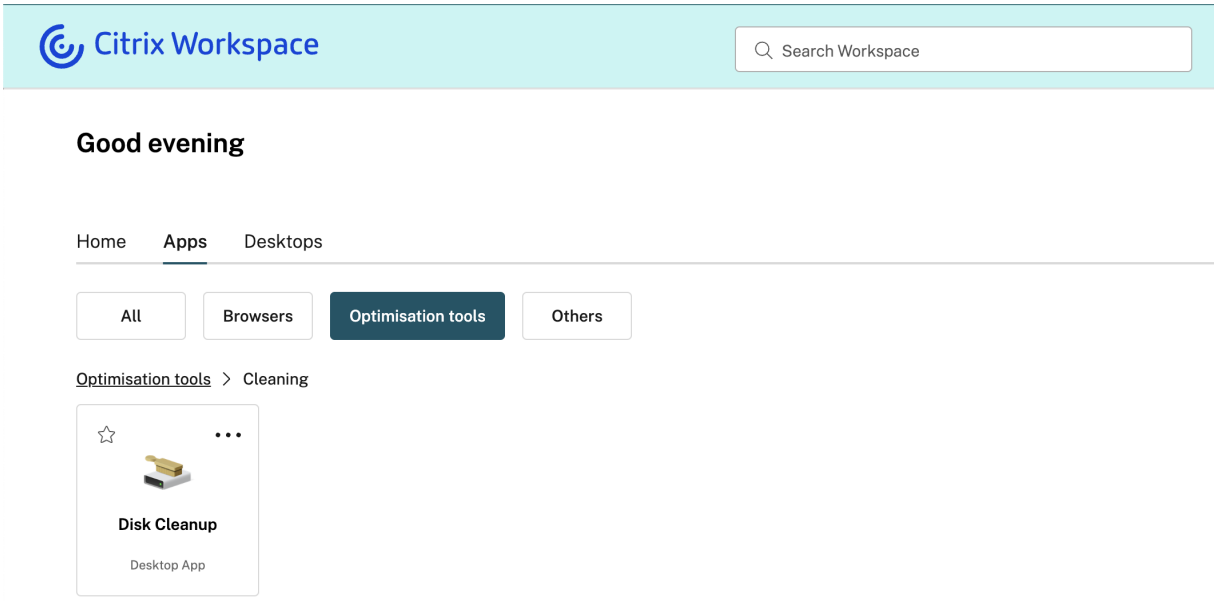


Select the relevant category, a list of available sub-categories and applications is displayed based on the configuration made by the admin.



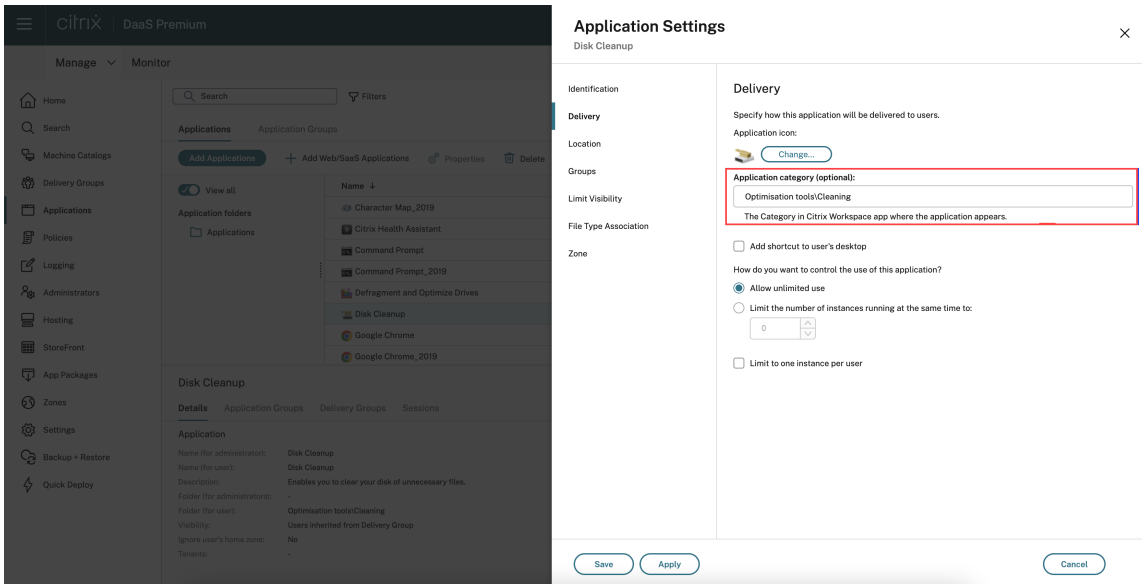
Add folder path

The folder path helps you define the categories under which an app appears. It represents the folder structure that appears on the screen for end users.
For example, consider an app for which the folder is defined as `Optimisation tools/Cleaning`. Now, to access this app, end users must go to Optimisation tools > Cleaning, where Optimisation tools is a category and Cleaning is it's sub-category.



To define the folder path for an application:

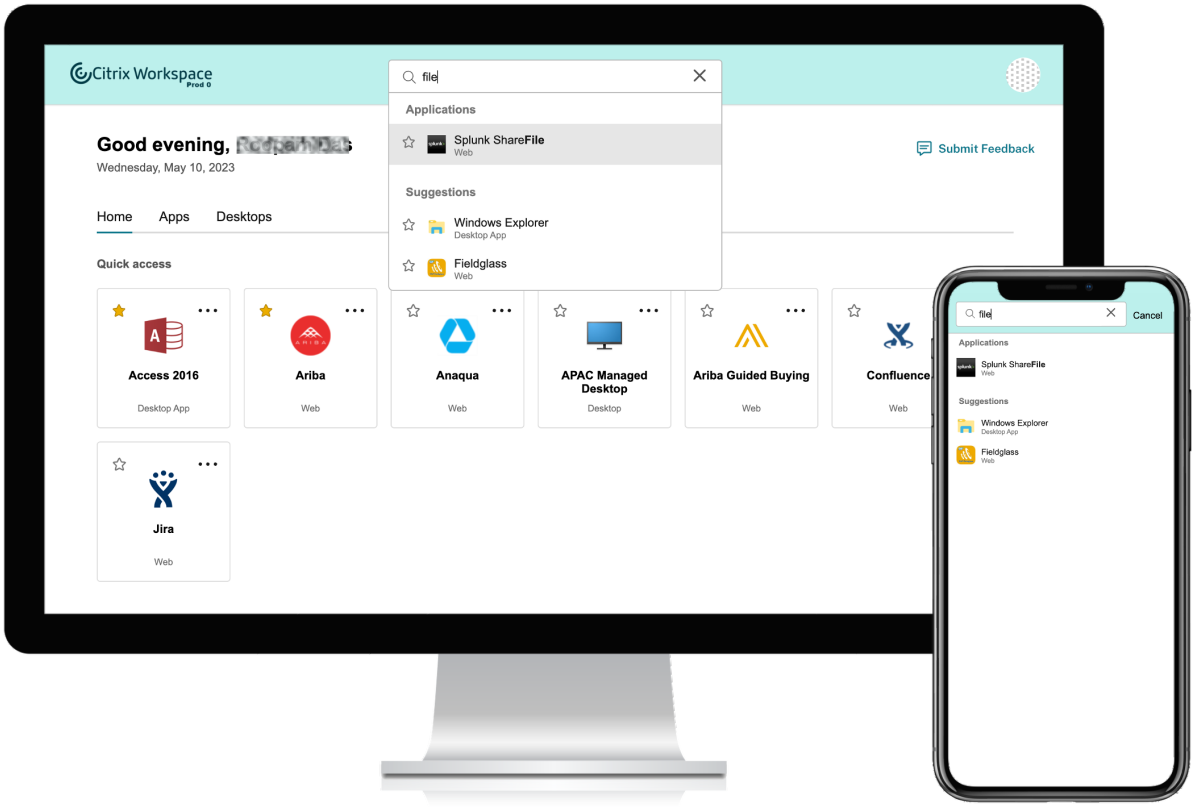
1. Navigate to **Citrix DaaS** on the admin cloud console.
2. Go to **Applications** and locate the app.
3. Right click on the app and select **Properties**.
4. In the **Application Category** field, define the folder path.



5. Click **Save**

Enhanced Search feature

The enhanced **Search** feature gives you faster results from the search engines. The **Search** option appears within the tool bar for ease of use, and allows you to do a quick and intuitive search from within the Workspace app.



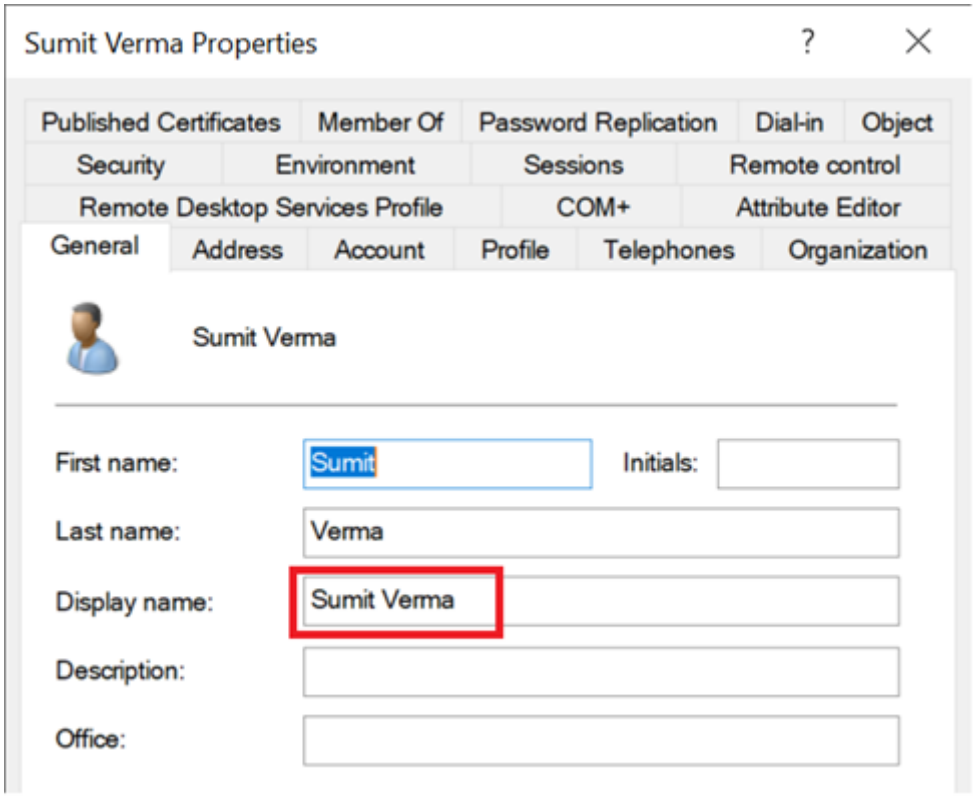
It includes the following improvements:

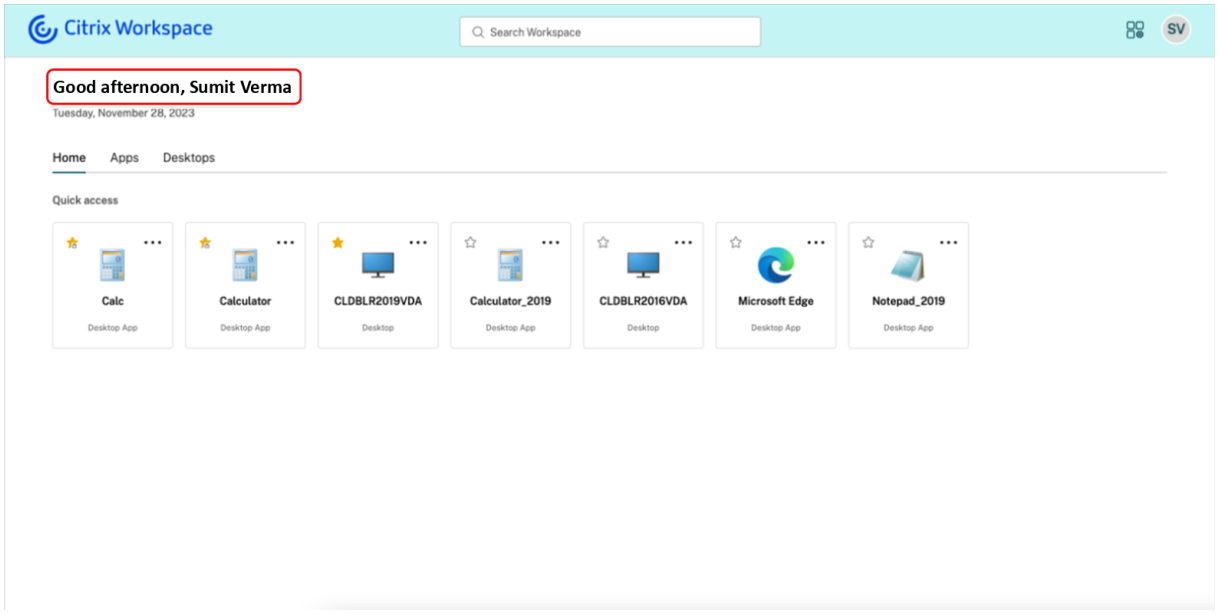
- Default search displays the five most recently used apps or desktops
- Searches are enabled with spell check, and display auto complete results
- Search results include apps within virtual sessions based on recently accessed, and Web and SaaS apps
- Perform search by admin created categories
- Search result lists **Favorites** at the top

Manage user's display name and profile picture

As an administrator, you can manage the appearance of the user's display name and profile picture on the Workspace UI starting from the release 23.48.

The user's display name is shown along with a greeting within the Workspace UI. The UI shows the user's display name only if the Active Directory (AD) user account contains a valid display name.

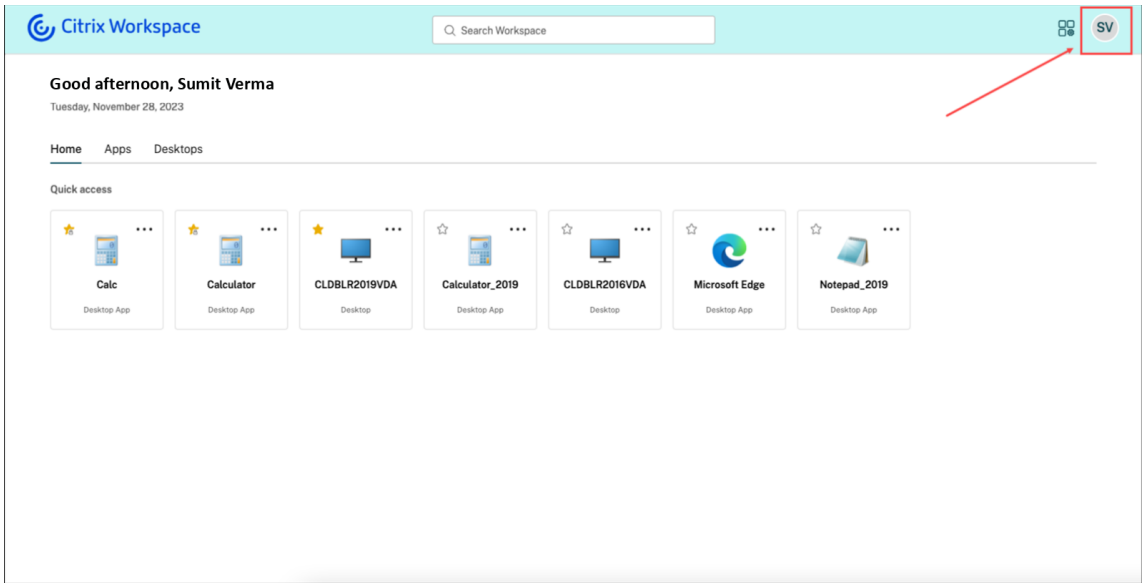




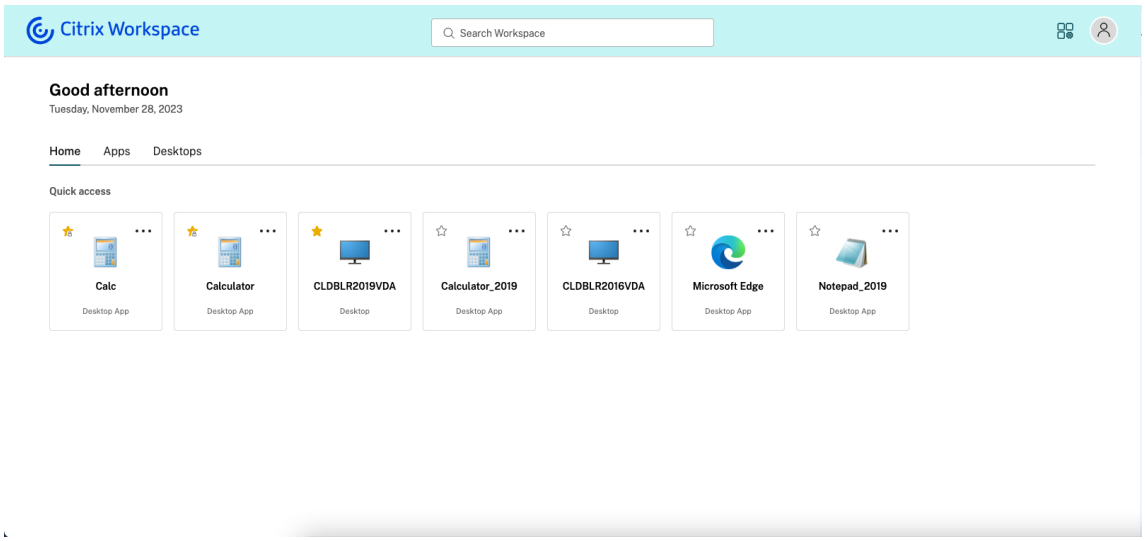
Users can see only the greeting if AD can't fetch a valid display name for the user.

Users can view their profile picture, initials, or a generic image depending on the following criteria:

- The user's profile picture is displayed if a picture is found in their AD user account.
- The user's initials are displayed if a picture can't be found but the AD successfully fetches the user's display name.



- A generic image is displayed if both the profile picture and the user's display name can't be fetched.



Troubleshooting an incorrect user's display name on Workspace UI

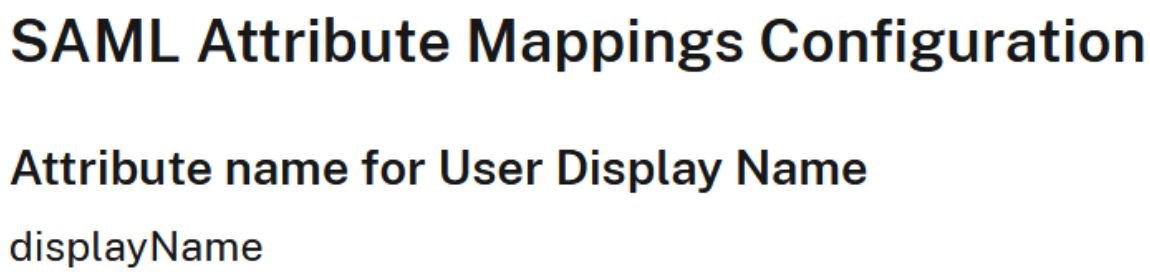
This section describes how to troubleshoot if users see a Security Identifier (SID) or Universally Unique Identifier (UUID) instead of the user's display name on Workspace UI.

The following are SAML scenarios that lead to an incorrect display name being shown within the Workspace UI:

Error Case 1: SAML Assertion is missing the displayName attribute The Workspace UI doesn't show the user's display name if you don't specify the `displayName` attribute within the SAML assertion. For more information on configuring SAML, see the following articles based on your Identity Provider (IdP):

- Configure SAML authentication in Citrix Cloud using ADFS
- Configure Okta as a SAML provider for Workspace authentication
- SAML using Azure AD and AD identities for Workspace authentication

Error Case 2: SAML Assertion contains the displayName attribute but it is incorrectly cased The `displayName` attribute is case-sensitive. You must send the correct attribute value and case within the SAML assertion, to display the user's display name correctly within the Workspace UI. It is the attribute that appears in the SAML assertion that matters, not the casing of any intermediate variables used by the SAML provider such as `user.displayname` (AAD example variable). What is specified in the SAML assertion should also match what is defined within the SAML Citrix Cloud connection.



Activity Manager

April 24, 2024

Activity Manager is a simple yet powerful feature in Citrix Workspace 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 disconnecting 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.

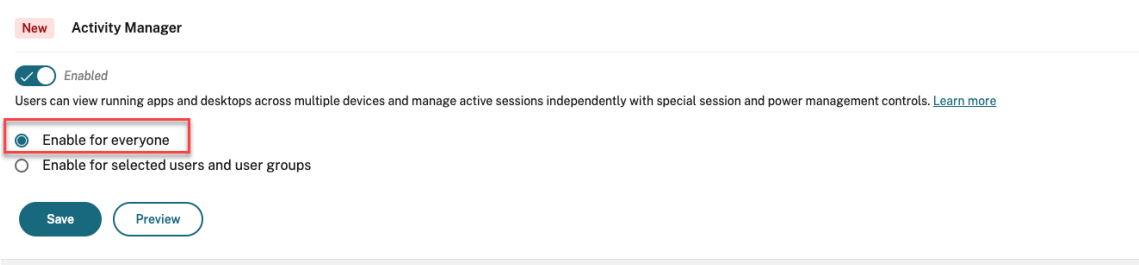
Enable Activity Manager

As an admin, you can now enable or disable the Activity Manager feature for your end users. As per your organization policies, you can enable the feature for everyone or selected users and user groups.

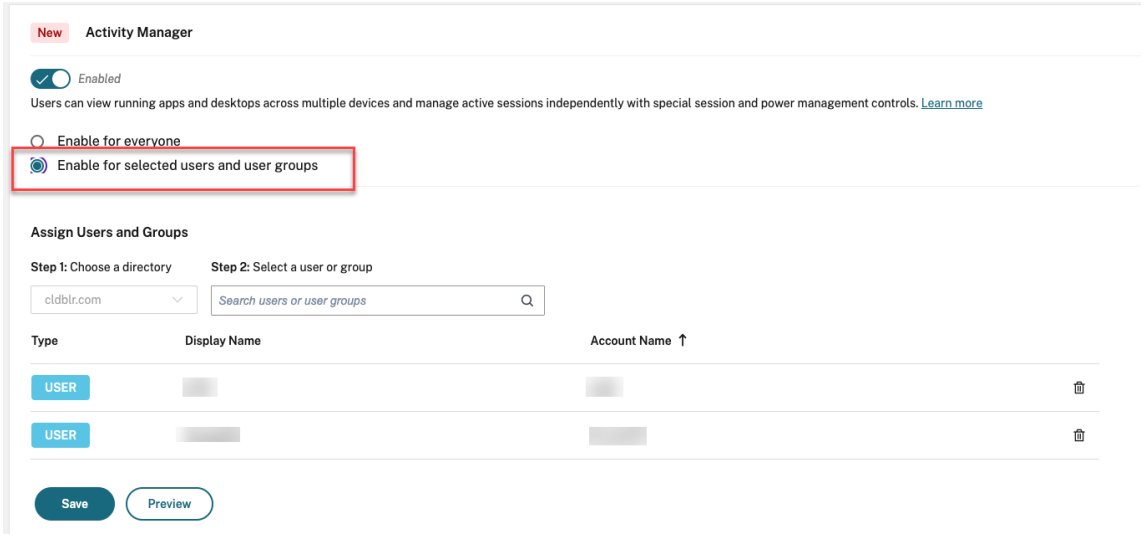
> **Note:**
>
> The Activity Manager feature can be enabled only for the new UI. For more information on the new UI, see Enable the new Workspace experience

To enable Activity Manager:

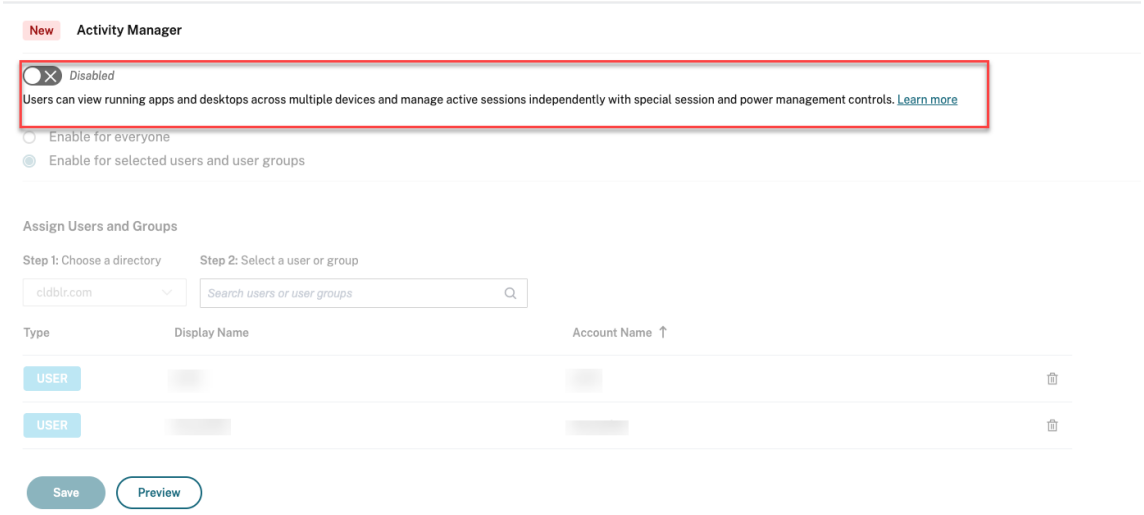
1. On the Admin console, go to **Workspace Configuration** > **Customize** > **Features**.
2. In the Activity Manager section, turn-on the toggle to enable Activity Manager.
3. You can then customize the access permissions as follows.
    - To enable Activity Manager for all end users, select **Enable for Everyone**.



    - To enable Activity Manager for selected users and user groups, select **Enable for selected user and user groups**. You can then select the directory to which the users or user groups belong. Once the appropriate directory is selected, you can view relevant users and user groups.



- To disable Activity Manager for everyone, turn-off the toggle.



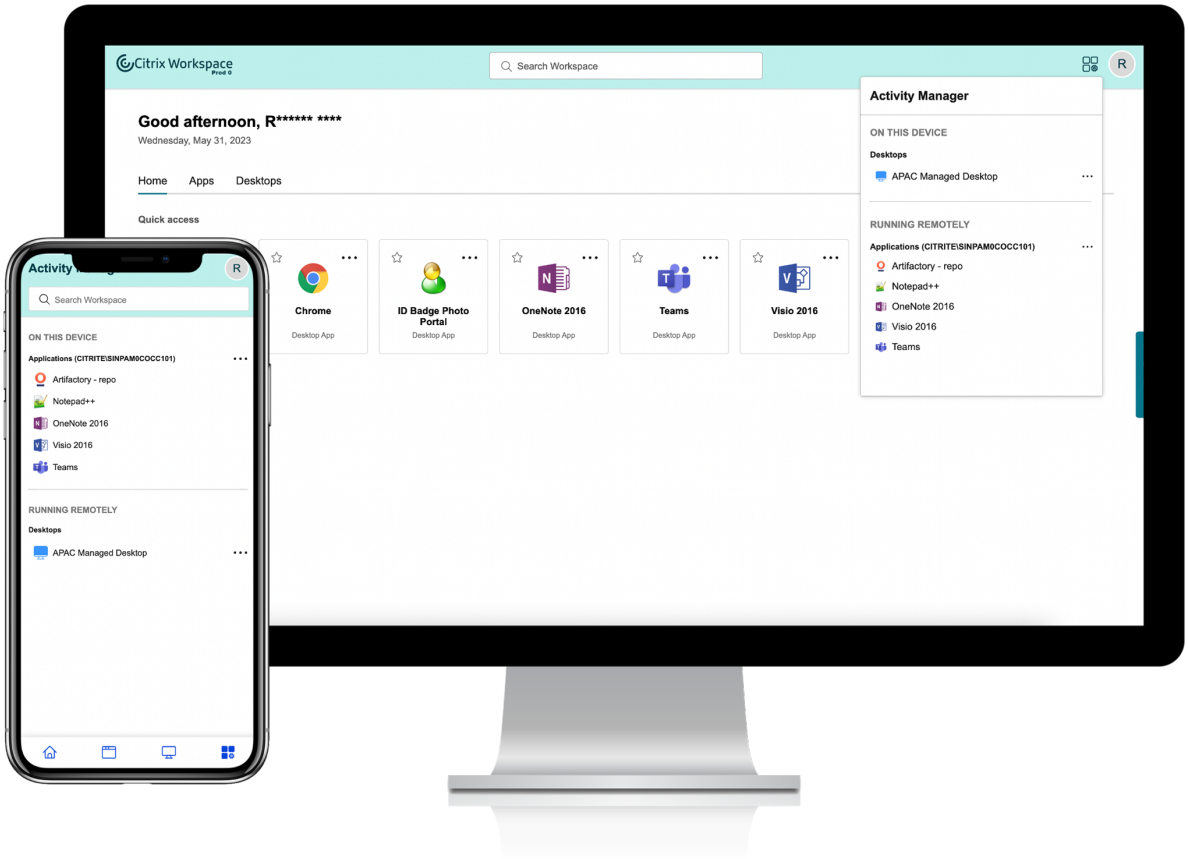
4. Click **Save**.

> **Note:**
>
> This feature is supported only for virtual apps and desktops. It is not applicable to web and SaaS apps.

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**.

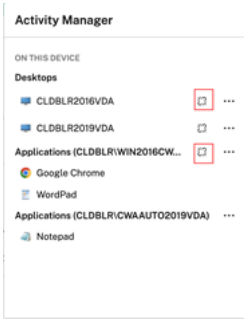


Users can perform the following actions on an app or desktop by clicking the respective ellipsis(…) button.

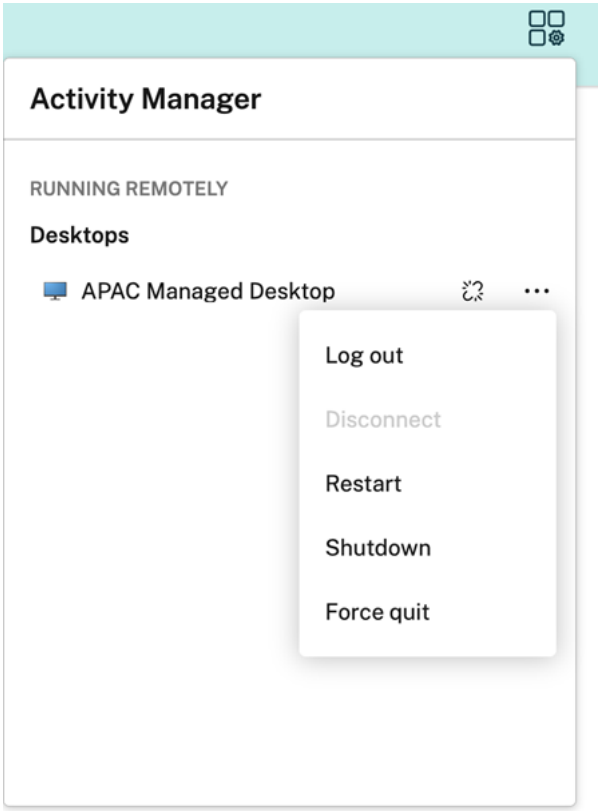
- **Disconnect**: The remote session is disconnected but the apps and desktops are active in the background.
- **Log out**: Logs out from the current session. All the apps in the sessions are closed, and any unsaved files are lost.
- **Shut Down**: Closes your disconnected desktops.
- **Force Quit**: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

Disconnected apps and desktops

Activity Manager now 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 you are signed into Citrix workspace through a browser, and disconnect a local session, the session is first displayed under On this device. However, once you close and reopen Activity Manager, the disconnected session is moved under Running Remotely.
- If you are signed into Citrix Workspace app through a native device, and disconnect a local session, the disconnected session disappears from the list. However, once you close and reopen Activity Manager again, the disconnected session is moved under Running Remotely.

Deliver DaaS and Virtual Apps and Desktops with Citrix Workspace

April 23, 2024

Citrix Workspace is the multitenant cloud service that replaces StoreFront, which is the single-tenant, on-premises app store that aggregates Citrix DaaS apps and desktops. The Citrix Workspace platform is the cloud component that provides the tools, services, and capabilities needed for remote working, extensibility, and customization through Citrix Workspace.

You have different options for aggregating your DaaS with Citrix Workspace. The option you choose depends on:

- Whether you want to fully migrate to the cloud or to adopt a hybrid solution.
- Whether you plan to allow external access to DaaS.

Full migration to the cloud

You can migrate your on-premises configuration to the cloud, allowing subscribers to access DaaS through Workspace, by moving your IT-managed infrastructure into a Citrix-managed environment. Full migration to the cloud means that there are fewer components for you to manage.

Citrix recommends that you use the Automated Configuration tool to simplify the migration process from one or more on-premises sites to a cloud service. The main steps involved in this process include the following:

1. Ensure that you meet the prerequisites for migrating your configuration.
2. Export your on-premises configuration. For information on this process, visit Exporting your Citrix Virtual Apps and Desktops on-premises configuration.

3. Import your configuration to the cloud. For information on this process, visit Importing your configuration to Citrix DaaS

For more information on Automated Configuration, visit Migrate to the cloud and the Tech Zone deployment guide.

Site aggregation for hybrid solutions

You can transition to Citrix Workspace with your existing on-premises Virtual Apps and Desktops deployment. This process is called site aggregation and involves substituting your IT-managed infrastructure with a Citrix-managed infrastructure.

You might choose site aggregation to slowly transition to Workspace, or if you want a hybrid solution that hosts some, but not all, components in the cloud. A hybrid model allows you to manage cloud capacity alongside on-premises resources and offers a unified end-user experience without fully migrating to the cloud.

Before you transition from StoreFront to Workspace with site aggregation, you must have an Active Directory (AD) configuration and Cloud Connectors installed in your resource locations.

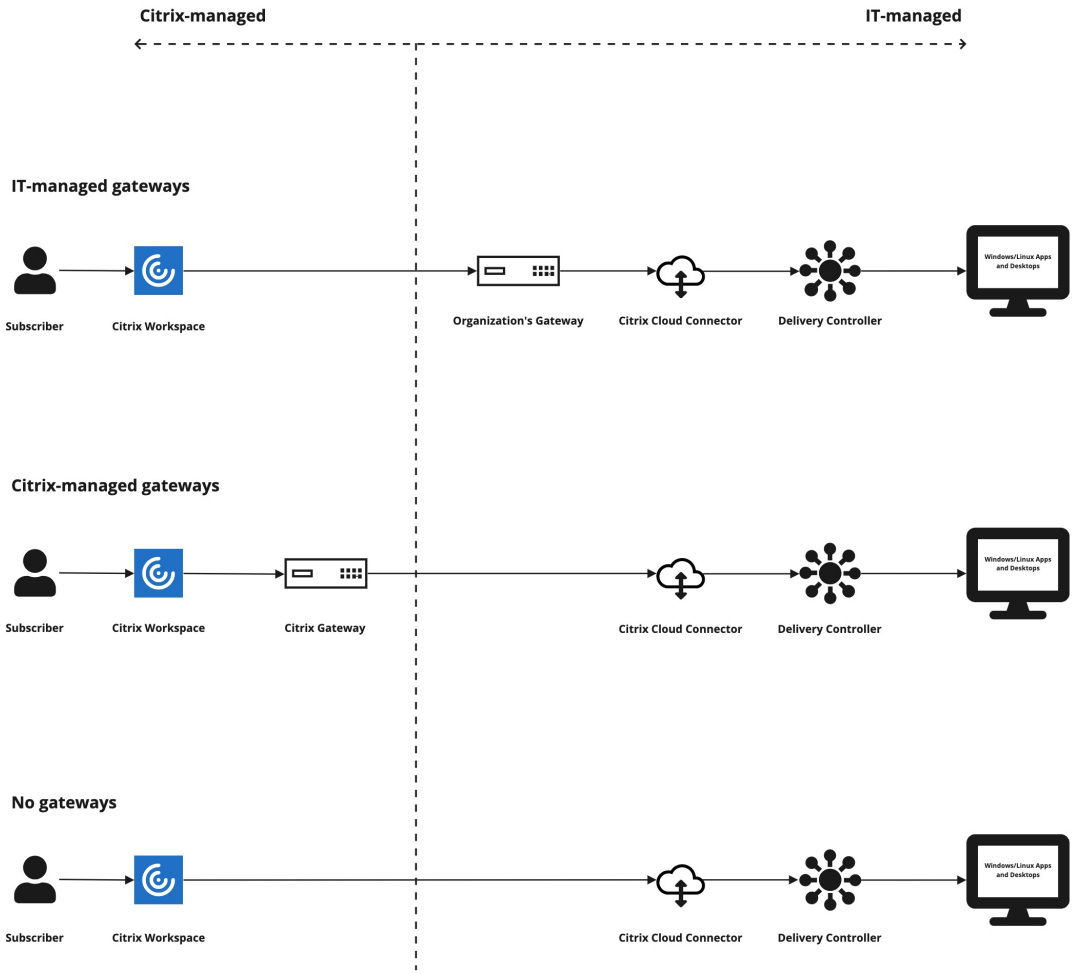
There are three broad steps involved in site aggregation:

1. **Discover site.** A site comprises the components that make up a production deployment. You might have different sites for different locations and branch offices.
2. **Verify Active Directory (AD) connection.** Subscribers must authenticate to Citrix Workspace with AD. Ensure that subscribers can authenticate by detecting the AD domains in which your Cloud Connectors are installed.
3. **Choose deployment type.** There are three connectivity options for this step:
    - IT-managed gateways
    - Citrix-managed gateways
    - No gateway

For more information, see Connectivity options.

Connectivity options

The following three options provide access to DaaS through Citrix Workspace, designed for different business requirements.



Connectivity option	Scenario
Traditional (IT-managed) gateways	Choose this option if you would like to use your own gateway for external connectivity to your DaaS. This allows you to take advantage of your current investment in on-premises gateways.
Citrix-managed gateways	Choose this option if you would like to use the **Citrix Gateway service** for external connectivity to your virtual apps and desktops. HDX connections between clients and VDAs are proxied through the **Citrix Gateway service**.

Connectivity option	Scenario
No gateway (internal only)	Choose this option if you want subscribers to launch to DaaS *only* using clients inside your corporate network. Subscribers won't have external access to DaaS if you choose this option.

For more information on the site aggregation process and the steps involved, visit Aggregate on-premises virtual apps and desktops in workspaces.

Configure workspace resiliency and optimization

For information on improving the efficiency and availability of your DaaS through Citrix Workspace, visit Optimize DaaS in Citrix Workspace. Citrix provides instructions 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).

Configure access to workspaces

February 19, 2024

Citrix recommends using the latest version of Citrix Workspace app to access workspaces. Citrix Workspace app replaces Citrix Receiver. You can also access workspaces using the latest version of Microsoft Edge, Google Chrome, Mozilla Firefox, or Apple Safari with the Workspace URL.

This article summarizes the steps involved in configuring and using:

- The Workspace URL
- The Citrix Workspace app (formerly Citrix Receiver).
- Citrix Gateways or the Citrix Gateway service for external connectivity.
- Identity providers for authentication to workspaces.

Overview

Subscribers can access Citrix Workspace through a browser with the Workspace URL or through the Citrix Workspace app installed on their devices.

The Workspace URL is customizable and is enabled by default. For instructions on editing the Workspace URL, see Workspace URL in this article.

Citrix Workspace app replaces Citrix Receiver as the natively installed app that provides access to the Workspace user interface (UI). For information about the Citrix Workspace app and transitioning from Citrix Receiver, see Citrix Workspace app (formerly Citrix Receiver) in this article.

Remote subscribers can gain external access to their workspaces if you configure external connectivity with Citrix Gateway or the Citrix Gateway service. For information on enabling remote access to workspaces, see External connectivity in this article.

Alternatively, for internal connectivity only, you can use Citrix Workspace on its own or host StoreFront on-premises. For internal connectivity, the endpoint must connect directly to the IP address of the Virtual Delivery Agent (VDA).

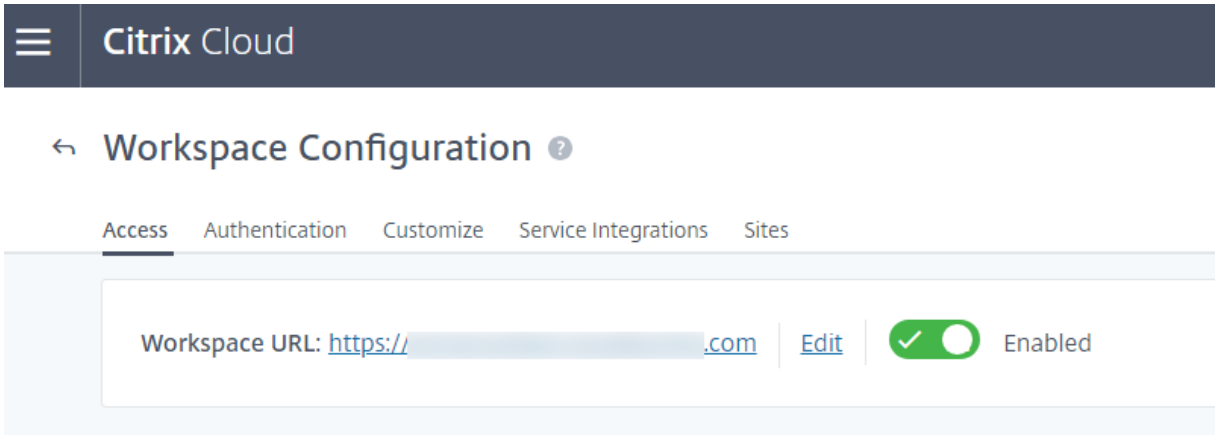
Citrix Workspace supports a growing list of identity providers that you connect to Citrix Cloud and then enable in **Workspace Configuration** to authenticate subscribers to their workspaces. For information on configuring authentication for Workspace subscribers, see Authentication to workspaces in this article.

Citrix Workspace also supports the following authentication options:

- Tokens as a second factor of authentication for signing in to workspaces with Active Directory. For more information on setting up multifactor authentication (MFA) to workspaces, see Two-factor authentication.
- Citrix Federated Authentication Service (FAS) to provide single sign-on (SSO) to DaaS in Citrix Workspace. For more information on setting up SSO with FAS, see Enable single sign-on for Workspaces with Citrix Federated Authentication Service.

Workspace URL

The Workspace URL is ready to use and can be found in **Citrix Cloud > Workspace Configuration > Access**, where you can enable, edit, and disable your Workspace URL.



Customize the Workspace URL

The first part of the Workspace URL is customizable. For example, you can change the URL from `https://example.cloud.com` to `https://newexample.cloud.com`.

You can change the Workspace URL only when it's enabled. If the URL is disabled, you must re-enable it first.

To enable the Workspace URL, navigate to **Workspace Configuration > Access** and select the toggle to enable it. Re-enabling the Workspace URL can take up to 10 minutes to take effect.

The first part of the Workspace URL represents the organization using the Citrix Cloud account, and must comply with the Cloud Software Group End User Agreement. Misuse of third party intellectual property rights, including trademarks, might result in revocation and reassignment of the URL or suspension of the Citrix Cloud account.

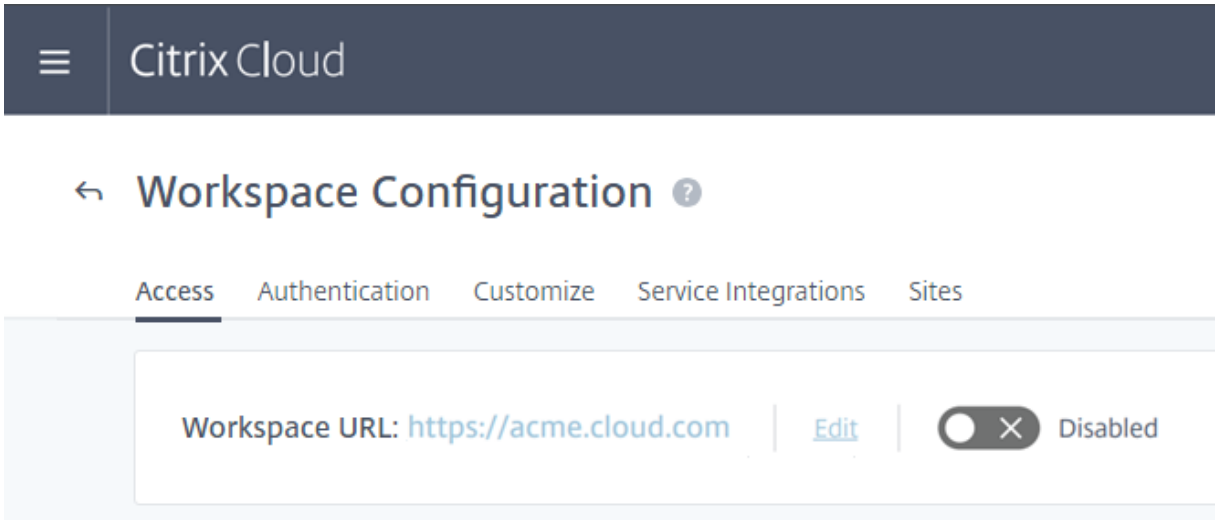
To customize your URL, go to **Workspace Configuration > Access** and select **Edit**. The customizable part of the URL:

- Must be between 6 and 63 characters long. If you want to change the customizable part of the URL to fewer than 6 characters, open a ticket in Citrix Cloud.
- Must consist of only letters and numbers.
- Can't include Unicode characters.

When you rename a URL, the old URL is immediately removed and is no longer available. Tell subscribers what the new URL is and manually update all local Citrix Workspace apps to use the new URL.

Disable the Workspace URL

You can disable the Workspace URL to prevent users from authenticating through Citrix Workspace. For example, you might want subscribers to use an on-premises StoreFront URL to access resources, or you might want to prevent access during maintenance.



Disabling the Workspace URL can take up to 10 minutes to take effect.

Disabling the workspace URL has the following effects:

- All service integrations are disabled. Subscribers can't access data and applications from services in Citrix Workspace.
- You can't customize the Workspace URL. You must re-enable the URL before you can change it.
- Anyone visiting the URL receives a message in their browser indicating that the workspace can't be found or that resources can't be loaded.

Citrix Workspace app (formerly Citrix Receiver)

> **Important:**
>
> Citrix Receiver has reached End of Life (EoL) and is no longer supported. If you continue to use Citrix Receiver, technical support is limited to the options described in Lifecycle Milestones and Definitions. For information about EoL milestones for Citrix Receiver by platform, refer to Lifecycle milestones for Citrix Workspace app and Citrix Receiver.

Citrix Workspace app is a natively installed app that replaces Citrix Receiver for accessing workspaces.

Supported authentication methods for Citrix Workspace app

The following table shows the authentication methods supported by Citrix Workspace app. The table includes authentication methods relevant to specific versions of Citrix Receiver, which Citrix Workspace app replaces.

Citrix Workspace app	Active Directory Authentication	Active Directory plus Token Authentication	Azure Active Directory authentication
Citrix Workspace for Windows	Yes	Yes	Yes (Workspace app; Receiver 4.9 LTSR CU2 and later only; Receiver 4.11 CR and later only)
Citrix Workspace for Linux	Yes	Yes	Yes (Workspace app; Receiver 13.8 and later only)
Citrix Workspace for Mac	Yes	Yes	Yes
Citrix Workspace for iOS	Yes	Yes	Yes
Citrix Workspace for Android	Yes	Yes	Yes (Workspace app; Receiver 3.13 and later only)

For more information about supported features in Citrix Workspace app by platform, refer to the Citrix Workspace app feature matrix.

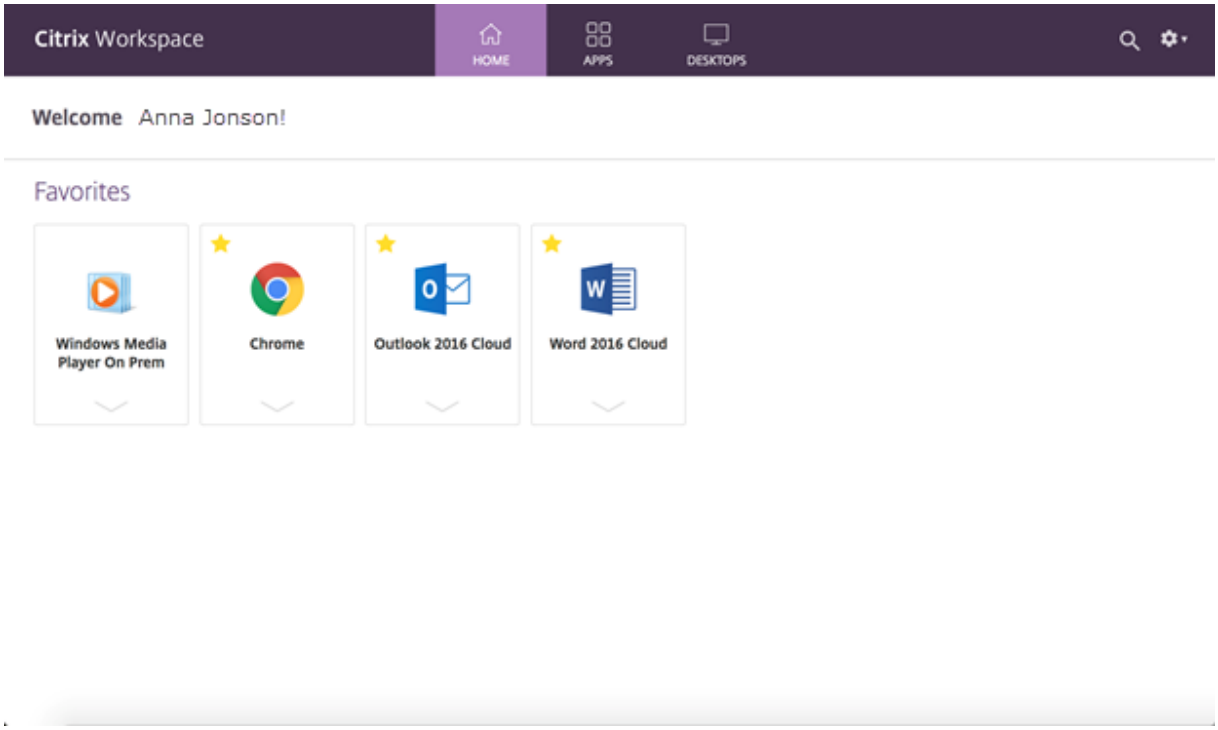
For an overview of TLS and SHA2 support with Citrix Receivers, see the CTX23226 Support article.

Transition from Citrix Receiver to Citrix Workspace app

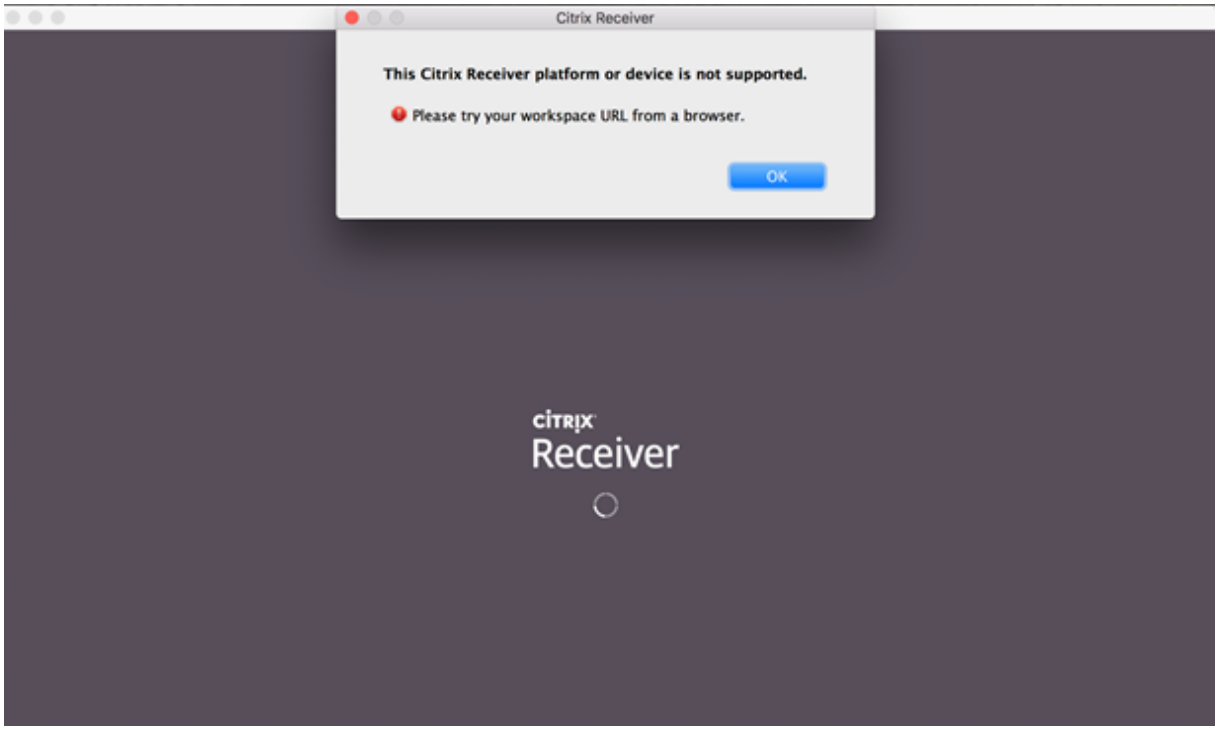
Citrix Workspace app replaces, and extends the capabilities of, Citrix Receiver.

Citrix Workspace app delivers access for subscribers to SaaS, Web, and virtual apps with a single sign-on (SSO) experience. For information on single sign-on for workspace subscribers, see Enable single sign-on for workspaces with Citrix Federated Authentication Service.

This access control feature isn't supported in Citrix Receiver. Thus, with the same services and access control enabled, Citrix Receiver users still see the purple UI, but without Web and SaaS apps. Additionally, **Files** isn't supported in Citrix Receiver and subscribers can't access them this way.



Azure Active Directory (AAD) also isn't compatible with Citrix Receiver. If subscribers attempt to access Workspace with Citrix Receiver when AAD is enabled as the authentication method, they see a message that the device isn't supported. Once they upgrade to Citrix Workspace app, they can access their workspaces.

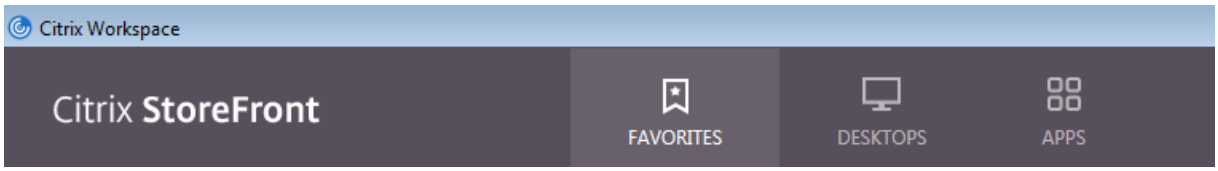


Customers that upgrade to Citrix Workspace app (or use a Web browser) see the new UI. For more in-

formation on what the subscriber experience of this UI is, visit Manage your workspace experience.

Aside from a new UI, the Citrix Workspace app allows subscribers to use all the new functionality that you've enabled. Subscribers can access **Files**, see DaaS, and access Web and SaaS apps through the Citrix Gateway service.

If you have a StoreFront (on-premises) deployment, upgrading from Citrix Receiver to Citrix Workspace app only changes the icon to open Citrix Workspace app.



> **Note:**
>
> Citrix Cloud Government users continue to see their purple UI when using the Citrix Workspace app or when accessing Workspace from a Web browser.

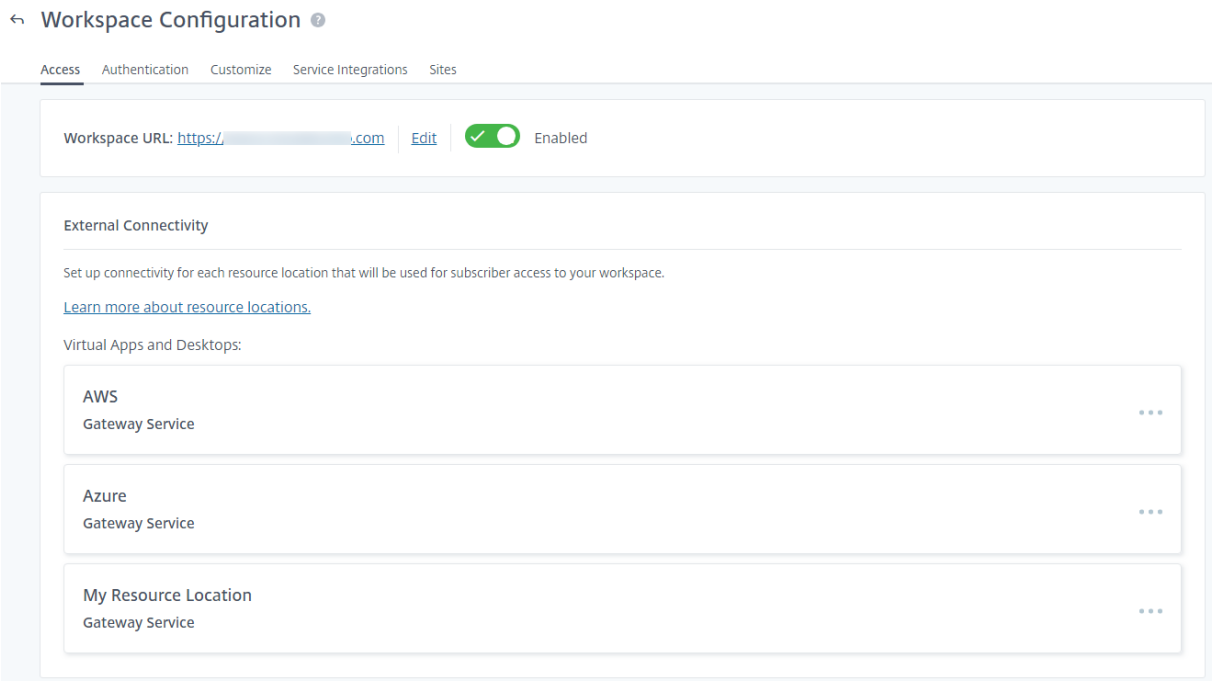
External connectivity

Provide secure access for remote subscribers by adding Citrix Gateways or the Citrix Gateway service to resource locations.

Citrix supports the following external connectivity options:

- Citrix hosts Citrix Gateway and Citrix ADC
- You host Citrix Gateway and Citrix ADC on-premises

You can add Citrix Gateways from **Workspace Configuration > Access > External Connectivity** or from **Citrix Cloud > Resource Locations**.



> **Note:**
>
> The External Connectivity part of the **Workspace Configuration > Access** page isn't available in Citrix Virtual Apps Essentials. The Citrix Virtual Apps Essentials service uses the Citrix Gateway service, which requires no additional configuration.

Authentication to workspaces

Configuring workspace authentication for subscribers is a two-step process:

1. Define one or more identity providers in **Identity and Access Management**. For instructions, visit Identity and access management.
2. Choose one of your configured identity providers as the authentication method used by subscribers to sign into their workspaces in **Workspace Configuration**. For instructions, visit Choose or change authentication methods.

Configuring more identity providers in **Identity and Access Management** gives you more options to choose from in **Workspace Configuration** for how subscribers sign into their workspaces.

Supported identity providers for authenticating subscribers

Subscribers can authenticate to their workspaces using one of the following methods:

- Active Directory
- Active Directory plus token

- Azure Active Directory
- Citrix Gateway
- Okta
- SAML 2.0
- Google

For more information on supported methods for subscriber authentication to workspaces, visit Secure workspaces.

Active Directory (AD) requires that you have at least two Citrix Cloud Connectors installed in the on-premises AD domain. For information about Citrix Cloud Connector, visit Citrix Cloud Connector.

AD plus Token is the default identity provider used to authenticate subscribers to workspaces. Subscribers generate tokens as a second factor of authentication using any app that follows the Time-Based One-Time Password (TOTP) standard, such as Citrix SSO. For information on setting up token-based two-factor authentication, see Two-factor authentication.

Changing identity providers

You choose an identity provider as your primary authentication method for Citrix Workspace in **Workspace Configuration**. The identity provider you choose must first be configured in **Identity and Access Management**. Changing the identity provider in **Workspace Configuration** doesn't affect the identity providers you've configured in **Identity and Access Management**.

Configuring identity providers in **Identity and Access Management** doesn't change the primary authentication method for signing into Citrix Workspace. To *change* the primary authentication method for signing into Citrix Workspace you must:

1. Configure the new identity provider in **Identity and Access Management**.
2. Change the identity provider in **Workspace Configuration**.

You can configure and change your primary authentication method for Citrix Workspace without breaking your production environment. If you'd like to test the new identity provider, you can either create a test Citrix Cloud organization or plan to change the authentication method in **Workspace Configuration** when subscribers aren't using their workspaces.

Single sign-on (SSO) to SaaS and Web apps

Citrix Workspace offers a seamless experience by providing single sign-on (SSO) to secondary resources once the subscriber has signed in to their workspace. Together with the Citrix Gateway service, Citrix Secure Private Access provides SSO to SaaS and Web apps as an integrated part of Citrix Workspace.

Beyond SSO capabilities, Citrix Secure Private Access allows you to set enhanced security policies, configure contextual access, and collect analytics. For more information about Citrix Secure Private Access, visit Citrix Secure Private Access.

Single sign-on (SSO) to DaaS

Alongside SaaS and Web apps, Active Directory (AD) and AD plus Token already provide SSO to DaaS apps and desktops after subscribers sign in to their workspaces.

If you select a different identity provider for the subscriber's initial authentication to Citrix Workspace, you might also install and configure the Citrix Federated Authentication Service (FAS). With FAS, subscribers enter their credentials only once to access their DaaS, just as they do with SaaS and Web apps.

FAS is typically adopted if you're using one of the following identity providers for Workspace authentication:

- Azure AD
- Okta
- SAML 2.0
- Citrix Gateway

> **Note:**
>
> 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.

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

More information

- Enable single sign-on for workspaces with Citrix Federated Authentication Service
- Reference Architecture: Federated Authentication Service
- Tech Insight: Federated Authentication Service

Configure a custom domain

April 17, 2024

Configuring a custom domain for your workspace 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.

A custom domain can't be shared with other Citrix Workspace customers. Each custom domain must be unique to that customer. Ensure that you choose the custom domain that you don't want to assign to another customer, unless you're willing to remove the custom domain later.

Disabling the Workspace URL within the Citrix Cloud doesn't disable Citrix Workspace access through the custom domain. To disable Citrix Workspace access when using a custom domain, also disable the custom domain.

Supported scenarios

Scenarios	Supported	Not supported
Identity providers	AD (+Token), Azure AD, Citrix Gateway, Okta, and SAML	Google
Resource types	Virtual Apps and Desktops	SaaS apps
Access methods	Browser (excluding Internet Explorer), Citrix Workspace app for Windows, Mac, Linux, and iOS apps	-
Usage	Workspace	Cloud Connector and Cloud Administrator Console

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 as a custom domain for Citrix Workspace access. It helps you change the domain easily, if necessary.
- Custom domains cannot contain any Citrix trademarks. Find the full list of Citrix trademarks here.
- 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.

> **Note:**
>
> Private DNS configurations are not supported.

- The length of the domain name must not exceed 64 characters.

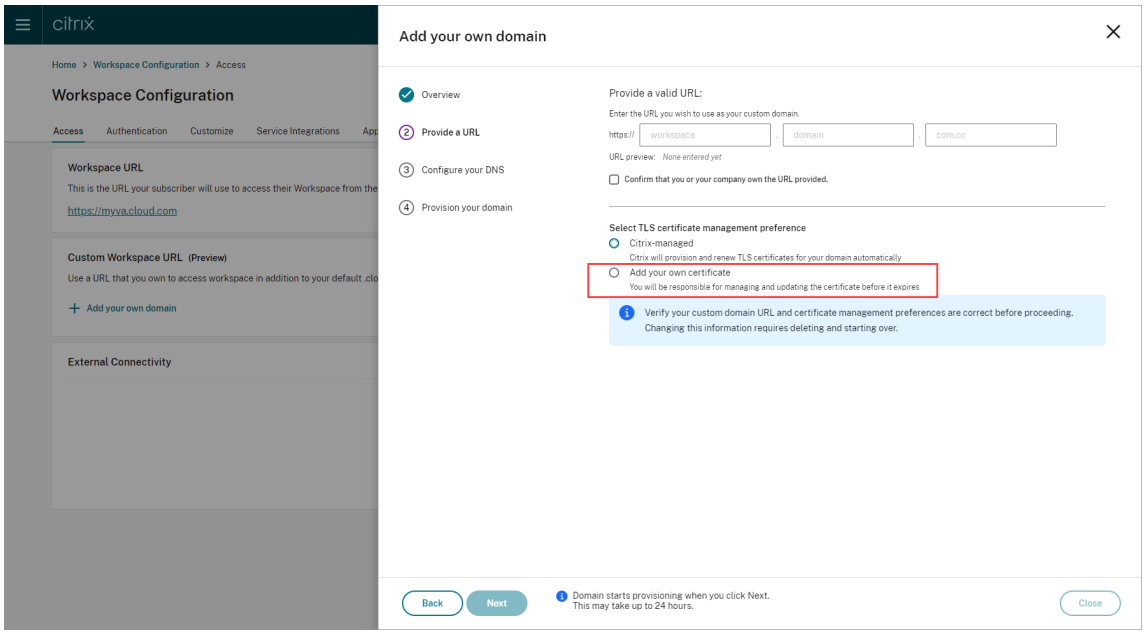
Configuring your custom domain

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.

If you're using SAML to connect to your Identity Provider, you need to perform an extra step to complete the SAML configuration. For more information, see SAML.

Adding a custom domain

1. Sign in to Citrix Cloud.
2. From the Citrix Cloud menu, select **Workspace Configuration** and then select **Access**.
3. On the **Access** tab, under **Custom Workspace URL** select **+ Add your own domain**.



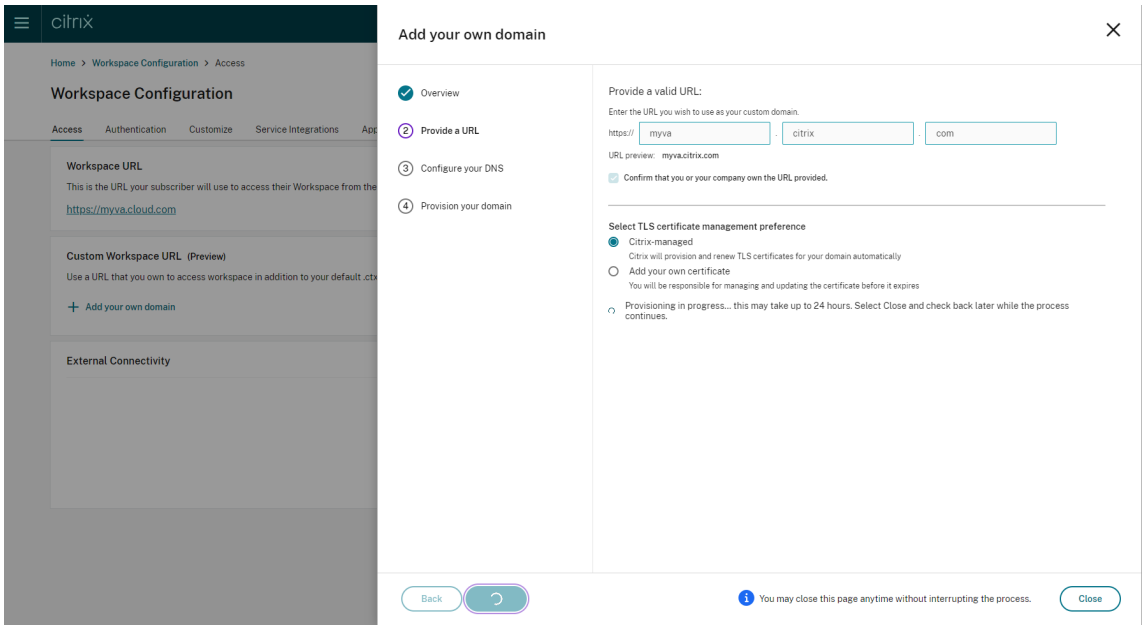
4. Read the information that appears on the **Overview** page, and select **Next**.
5. Enter your chosen domain in the **Provide a URL** page. Confirm that you own the specified domain by selecting **Confirm that you or your company own the URL provided**, and choose your

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**.

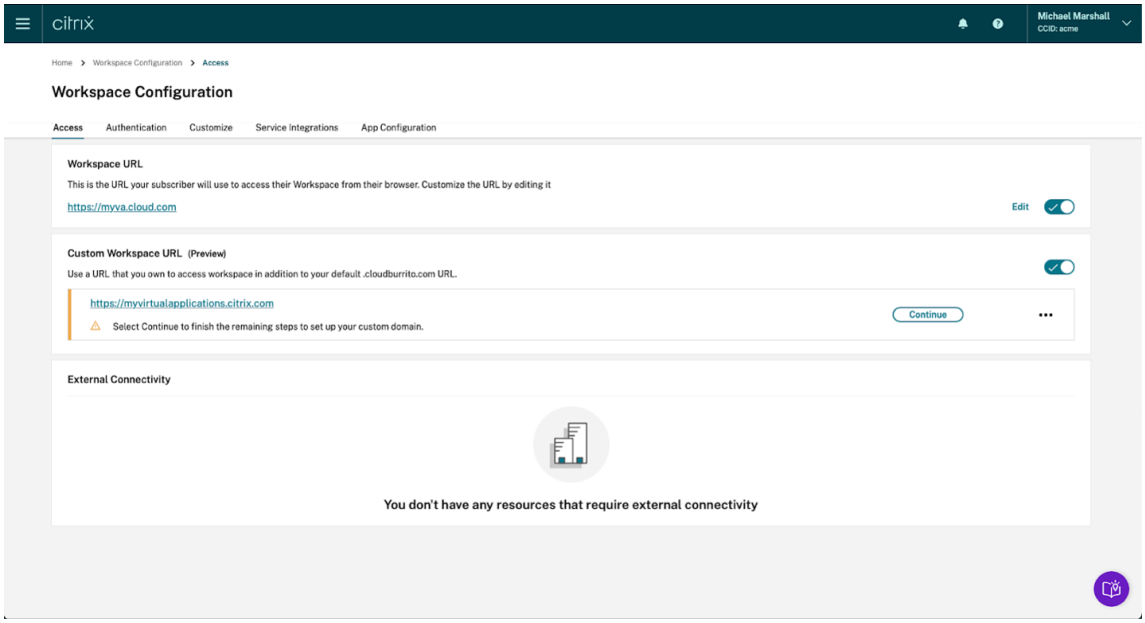
If any warnings appear on this page, correct the highlighted issue to proceed.

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.

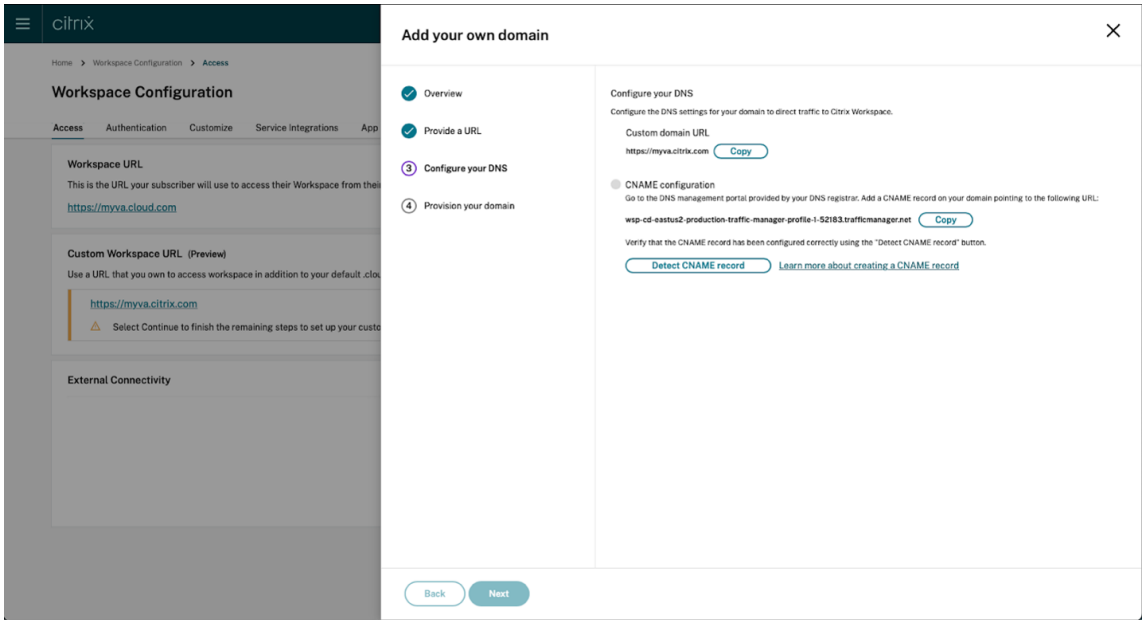


7. Perform this step in the management portal provided by your DNS registrar. Add a **CNAME** record for your chosen custom domain that points to the Azure Traffic Manager assigned to you.

   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-1-52183.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"*

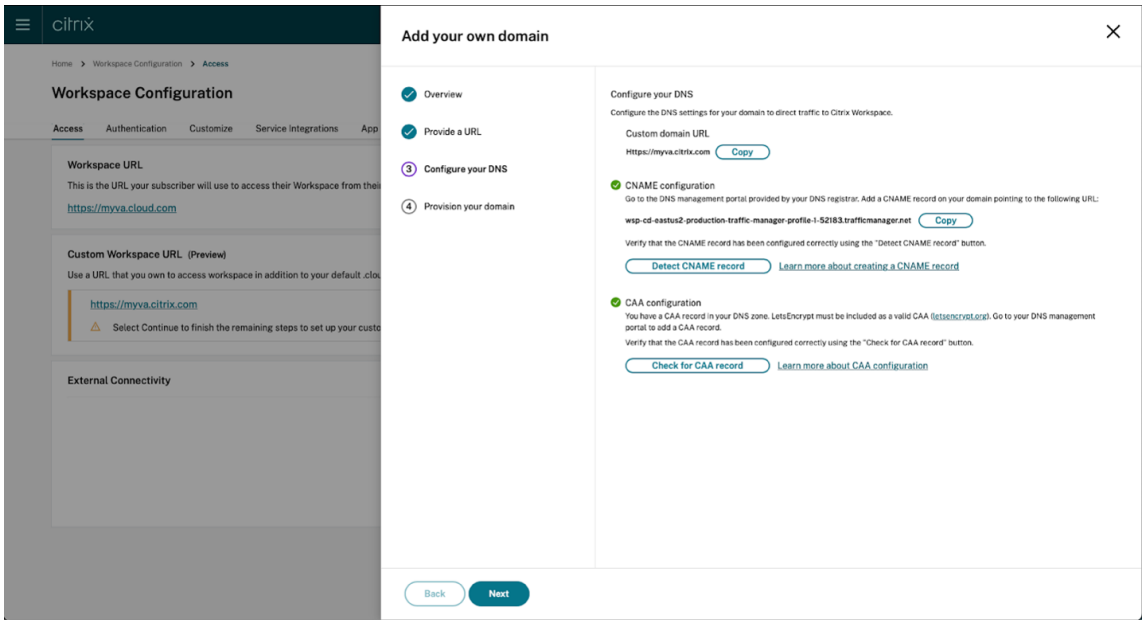


8. Once you configure the CNAME record with your DNS provider, select **Detect CNAME record** to verify that your DNS configuration is correct. If the CNAME record has been configured correctly, a green tick appears next to the **CNAME configuration** section.

   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**.

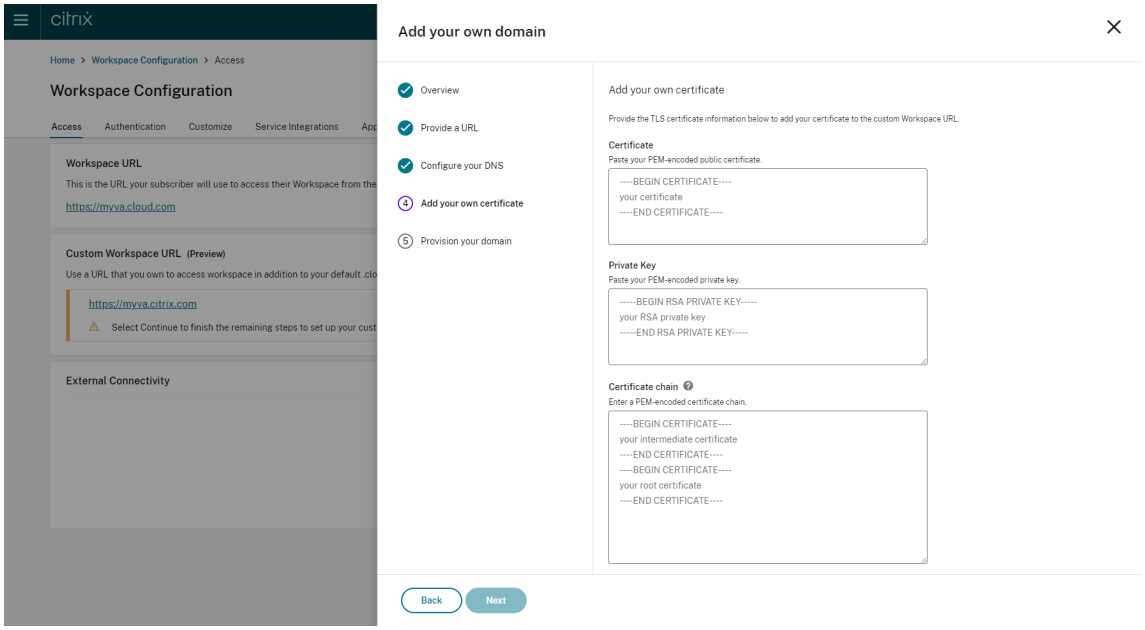


9. **This is an optional step**. If you chose to add your own certificate, complete the required information on the **Add your own certificate** page.

   > **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 Workspace 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.

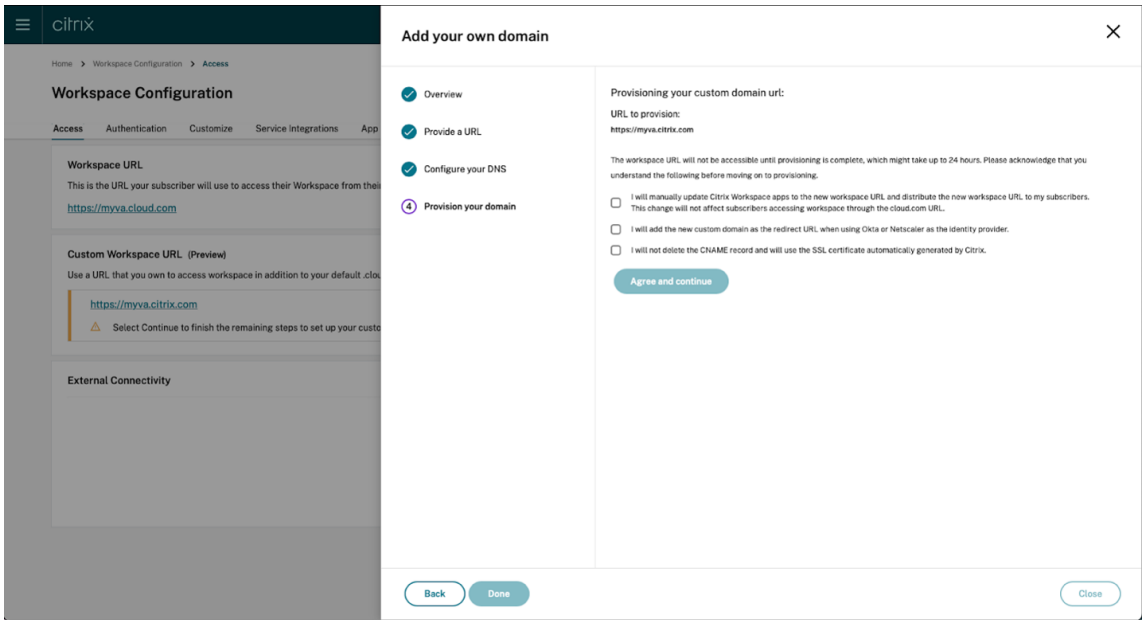
10. **This is an optional step.** If you're using SAML as your Identity Provider, supply the related configuration. Complete the required information on the **Configure for SAML page**.

    Use the following details when configuring the application in your Identity Provider:

Property	Value
Audience	`https://saml.cloud.com`
Recipient	`https://<your custom domain>/saml/acs`
ACS URL Validator	`https://<your custom domain>/saml/acs`
ACS Consumer URL	`https://<your custom domain>/saml/acs`
Single Logout URL	`https://<your custom domain>/saml/logout/callback`

11. 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.



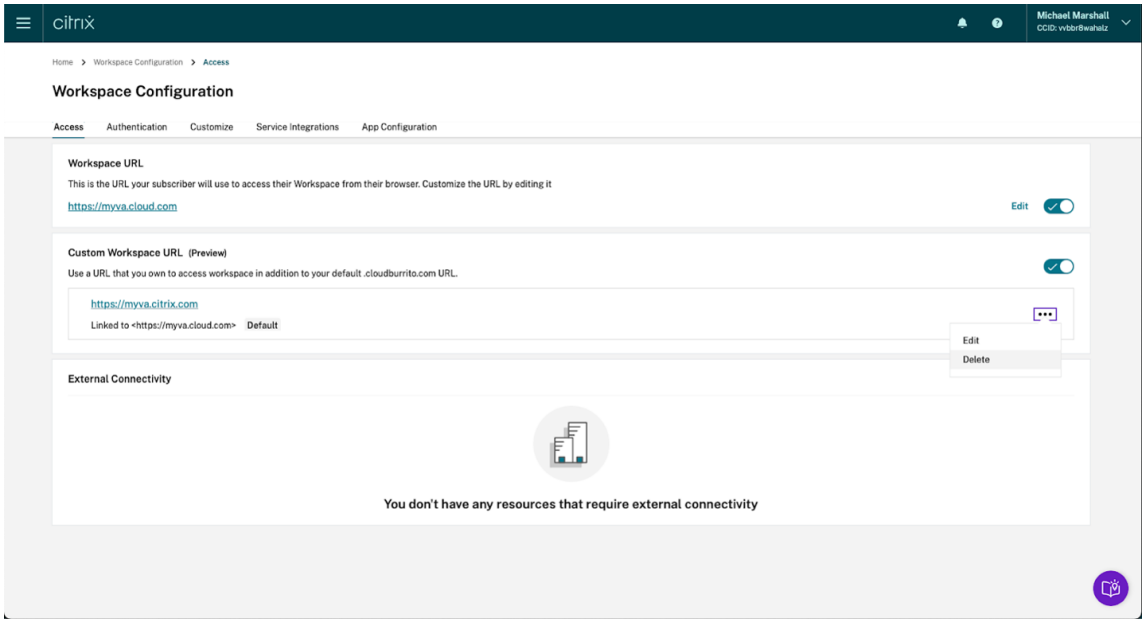
Deleting a custom domain

Deleting a custom domain from your customer removes the ability to access Citrix Workspace using a custom domain. After deleting the custom domain, you can only access Citrix Workspace using the cloud.com address.

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

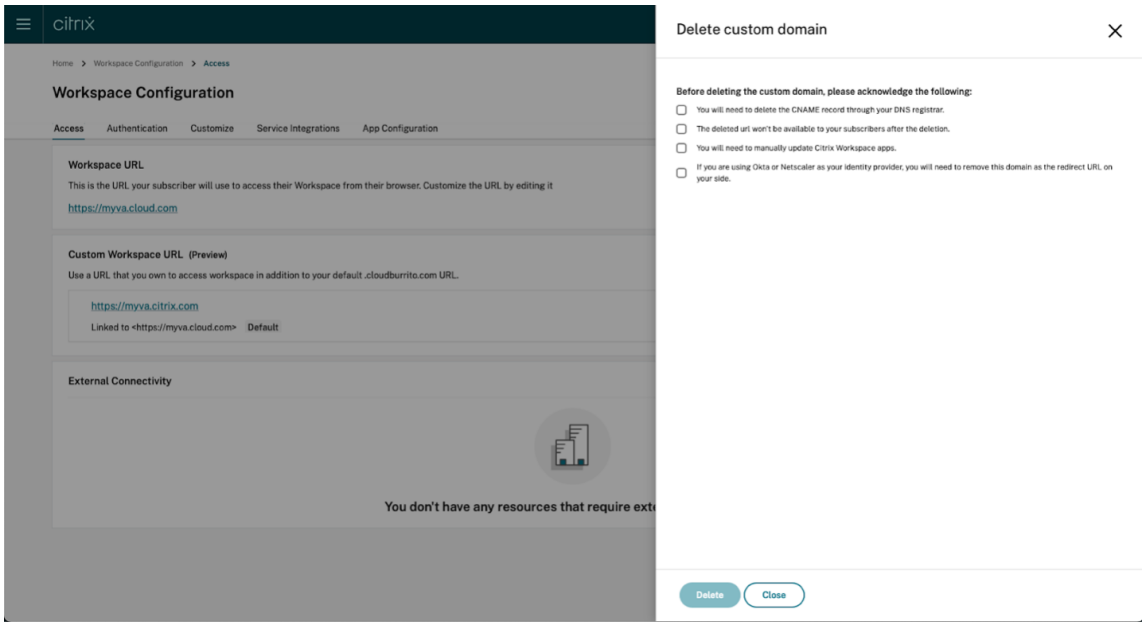
To delete a custom domain,

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



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**.

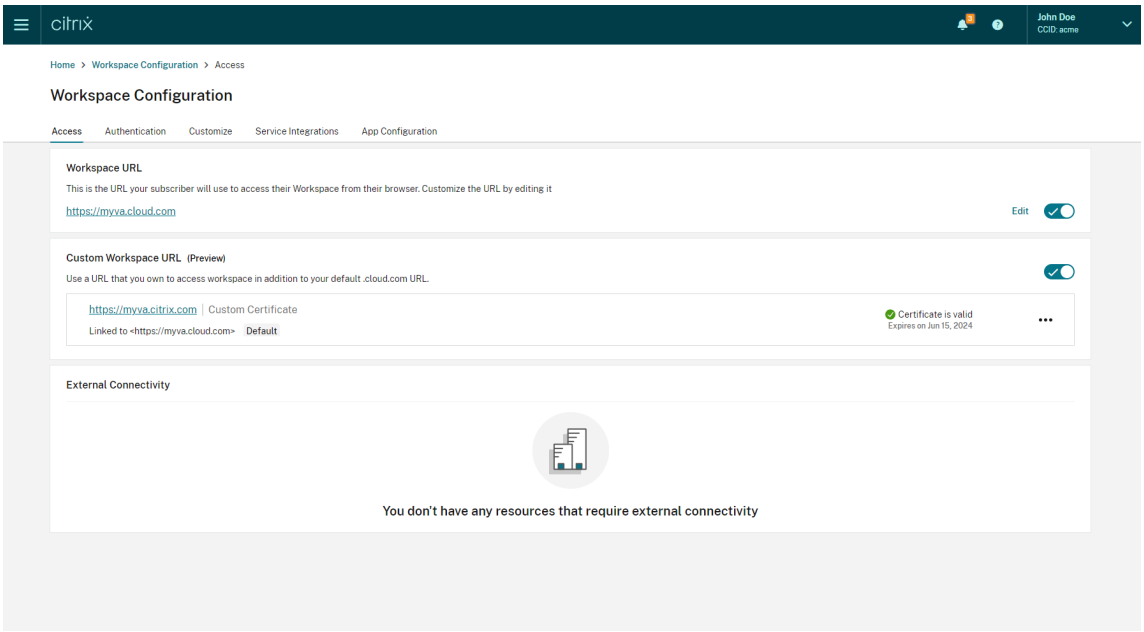
   Deleting a custom domain takes some time to complete. You can wait with the page open while the operation completes, or you can close the page.



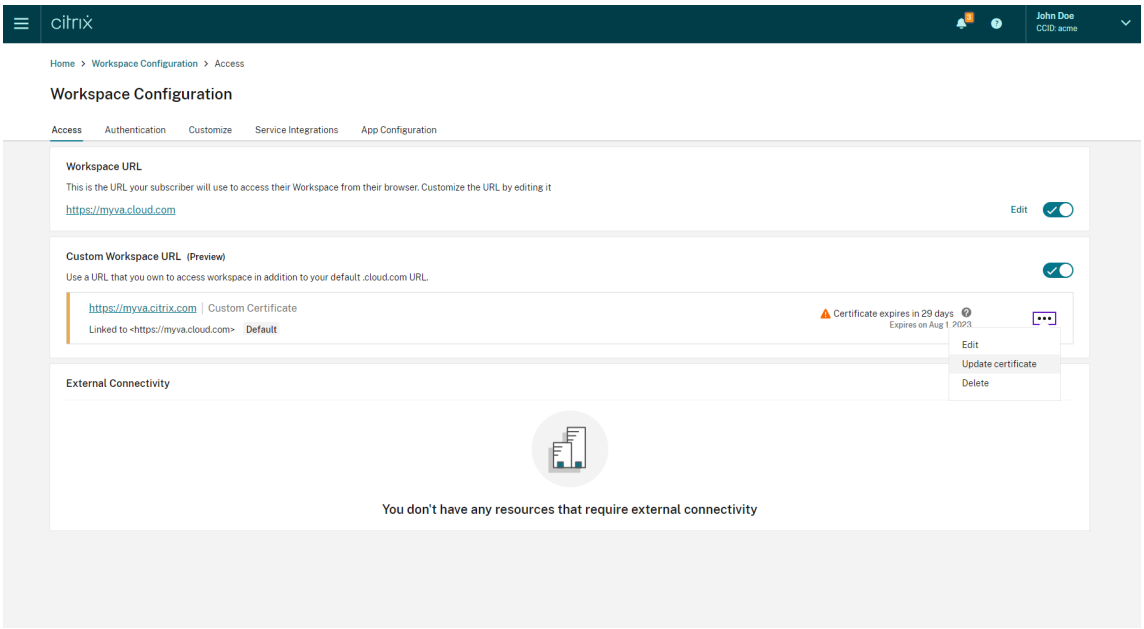
Providing a renewed certificate

1. Sign in to Citrix Cloud.
2. From the Citrix Cloud menu, select **Workspace Configuration** > **Access**.

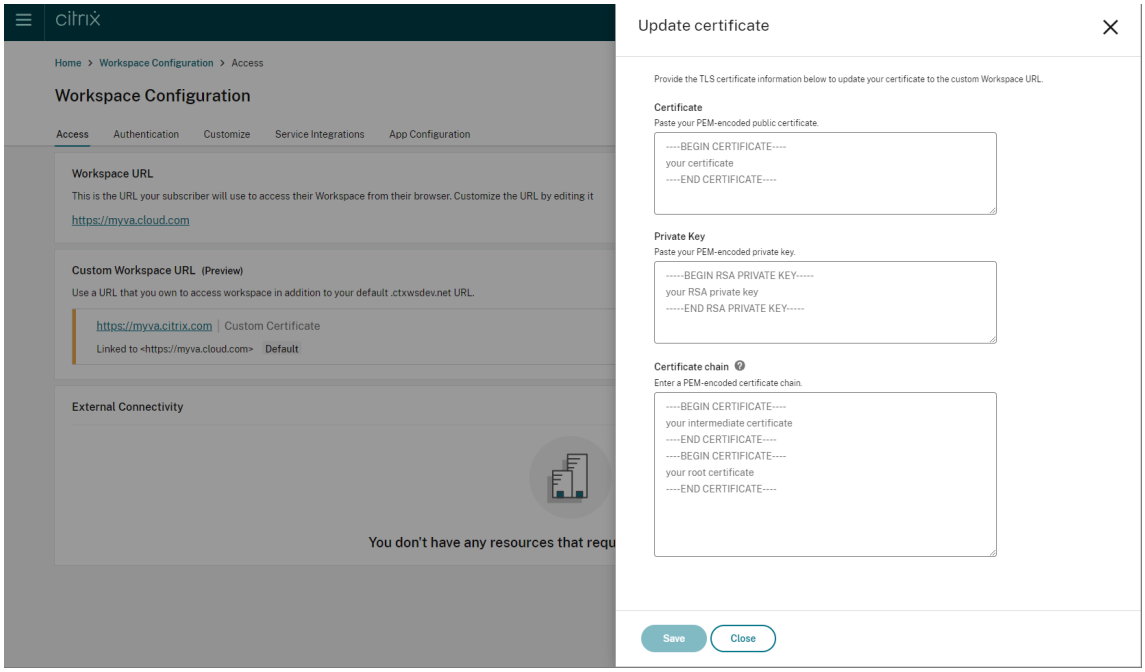
3. The certificate's expiration date is shown alongside the custom domain that it is assigned to.



When your certificate is about to expire in 30 days or less, your custom domain displays a warning.



4. Expand the context menu **(...)** for the custom domain on the **Access** tab. Select **Update certificate**.



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.

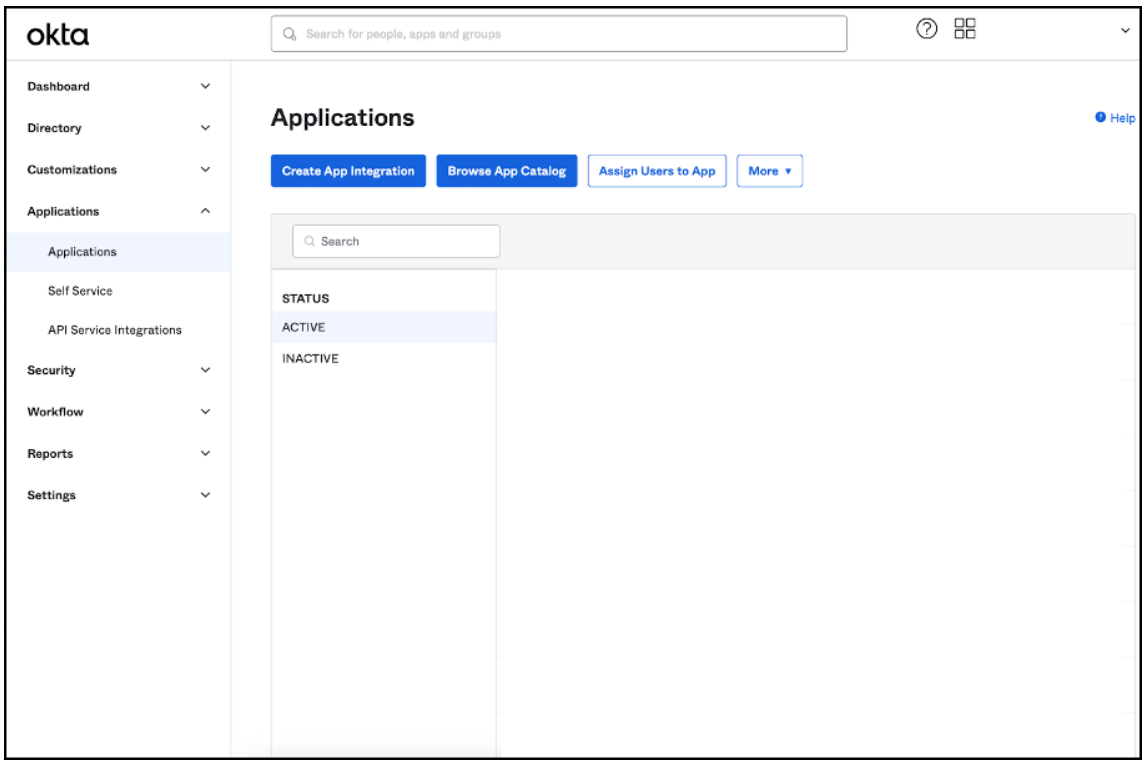
The certificate must meet the same requirements as when the custom domain was created. For more information, see Adding a custom domain.

Configuring your identity provider

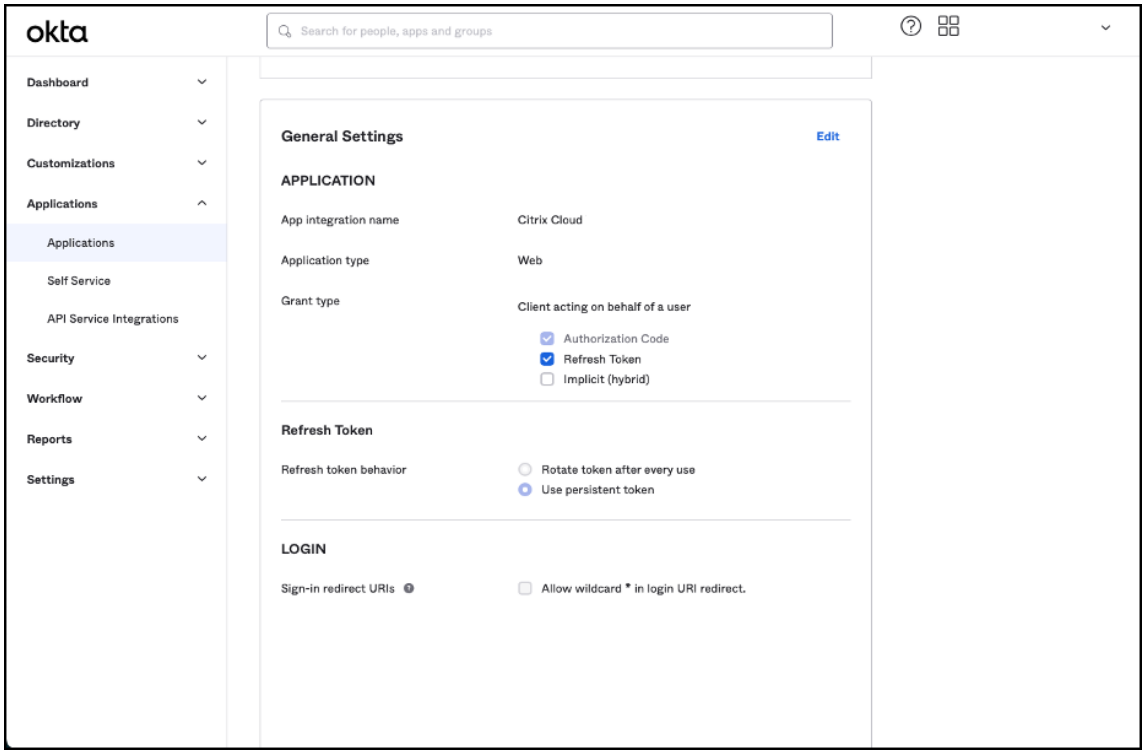
Configuring Okta

Perform the following steps if you are using Okta as the identity provider for Citrix Workspace 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.



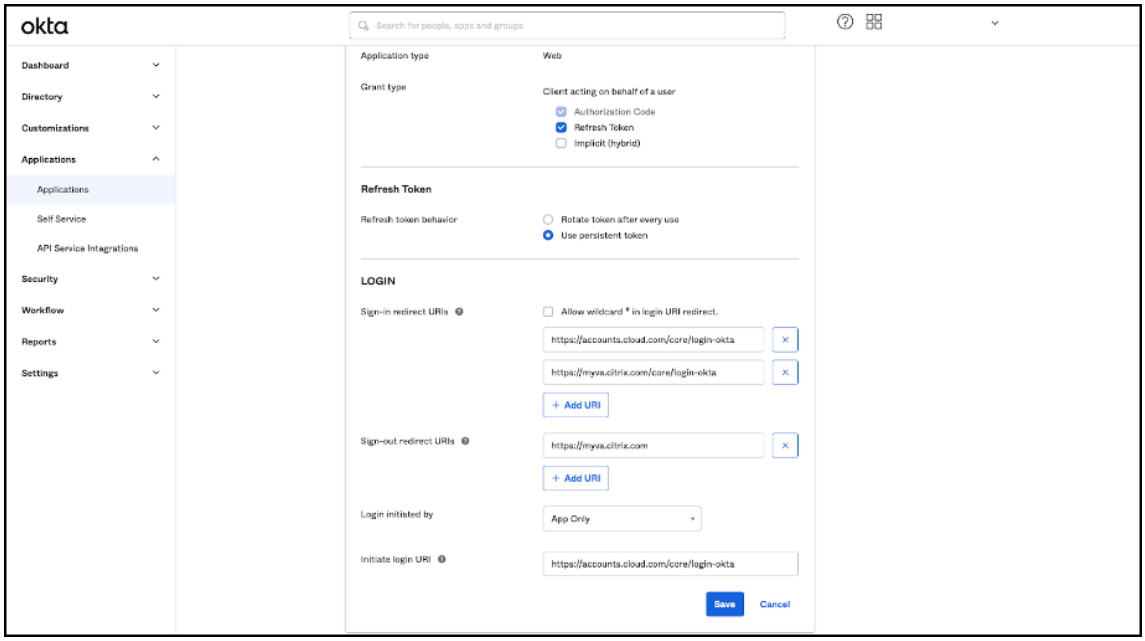
3. Open the application linked to Citrix Cloud.
4. Select **Edit** in the **General Settings** section.



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 Workspaces and affects your ability to log in to Workspaces.

Configuring Citrix Gateway

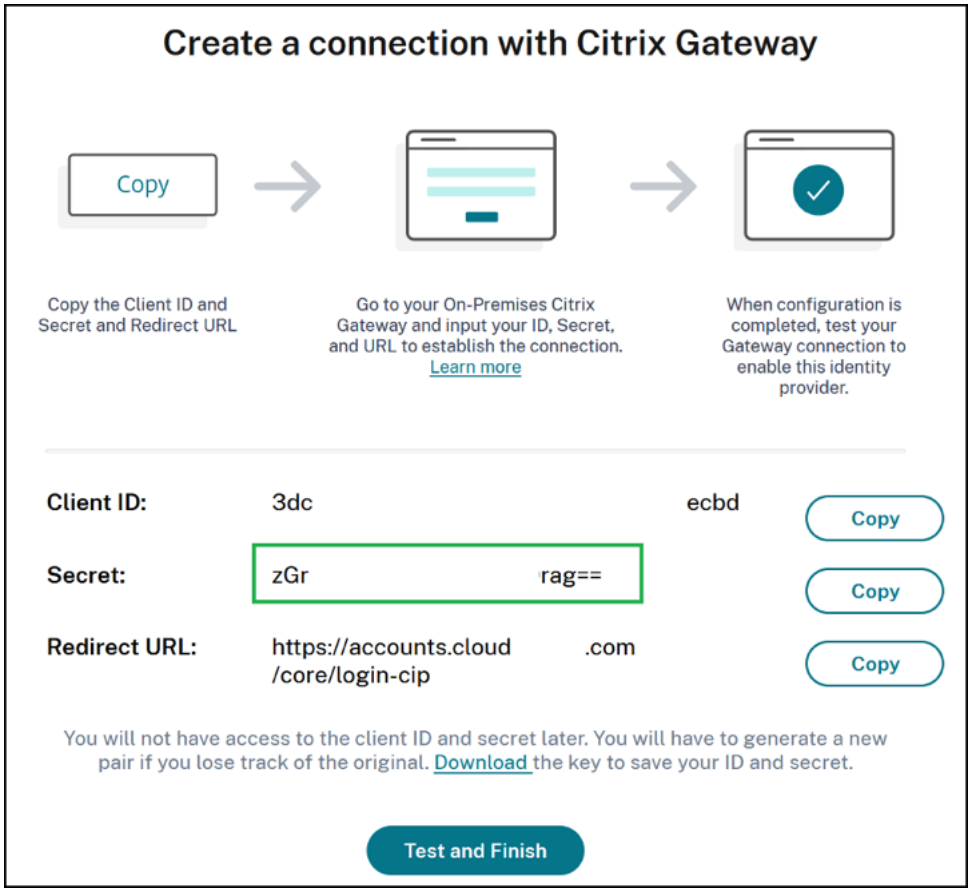
The Citrix Cloud admin has the access to the unencrypted client secret. These credentials are provided by Citrix Cloud during the Citrix Gateway linking process within **Identity and Access Management >**

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.

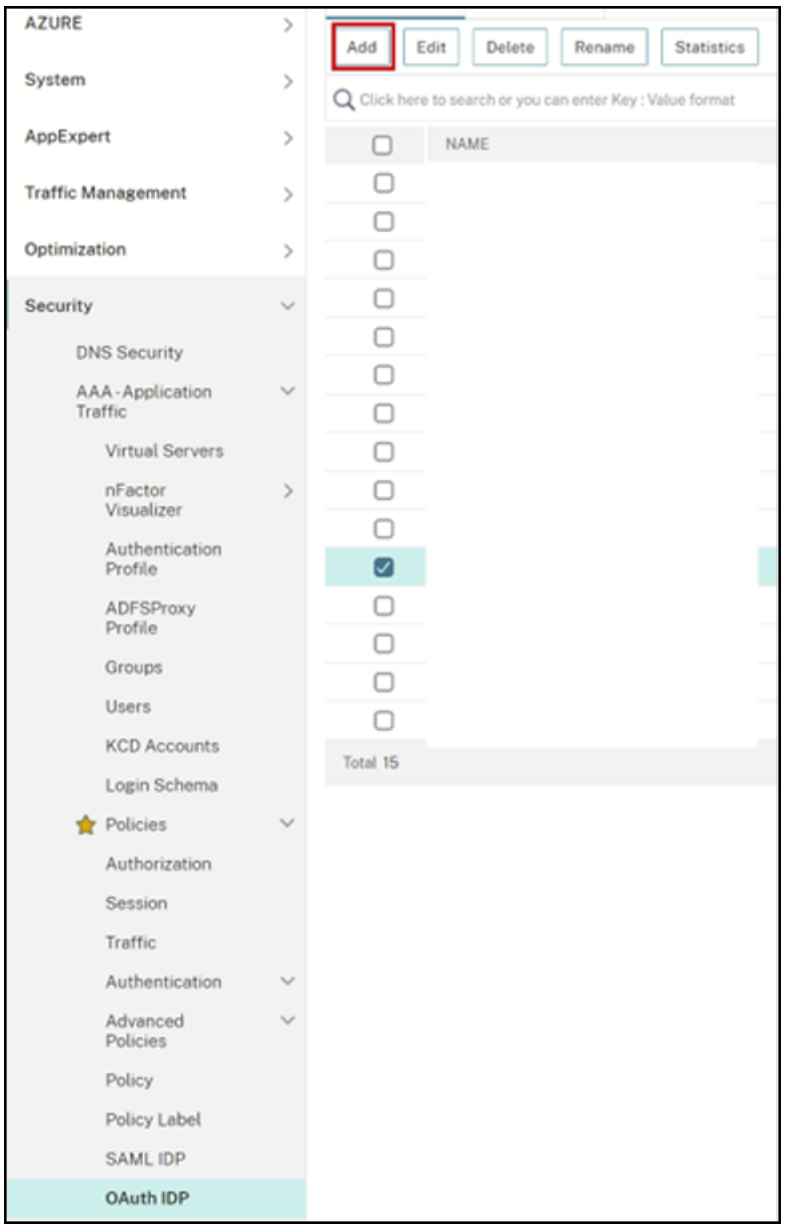
Here's an example of the UI when the client ID and secret are provided to the Citrix Admin.

> **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.

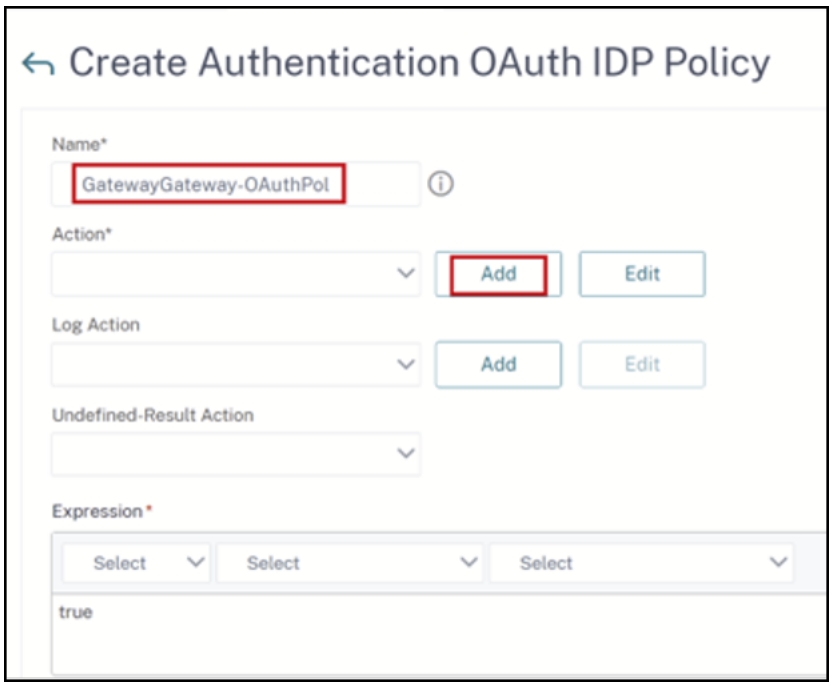


Using Citrix Cloud Perform these steps to add another OAuth profile and policy using the Citrix Gateway interface:

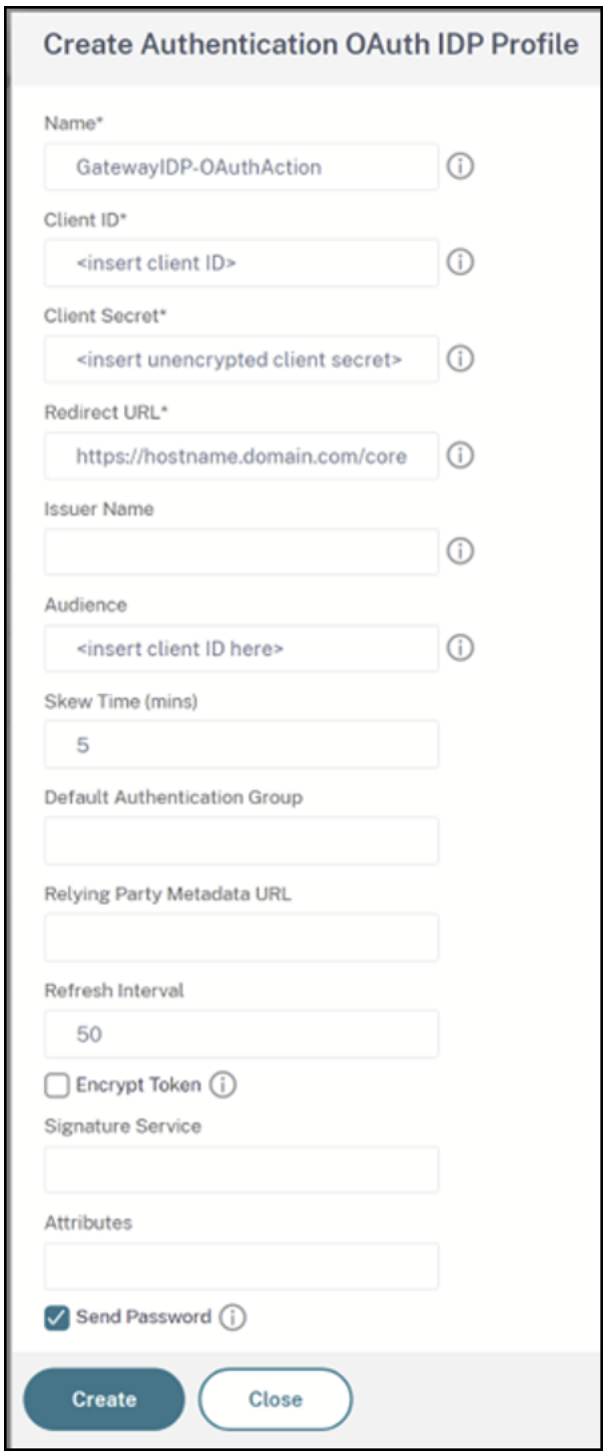
1. From the menu select **Security > AAA - Application Traffic > OAuth IDP**. Select the existing OAuth policy and click **Add**.



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

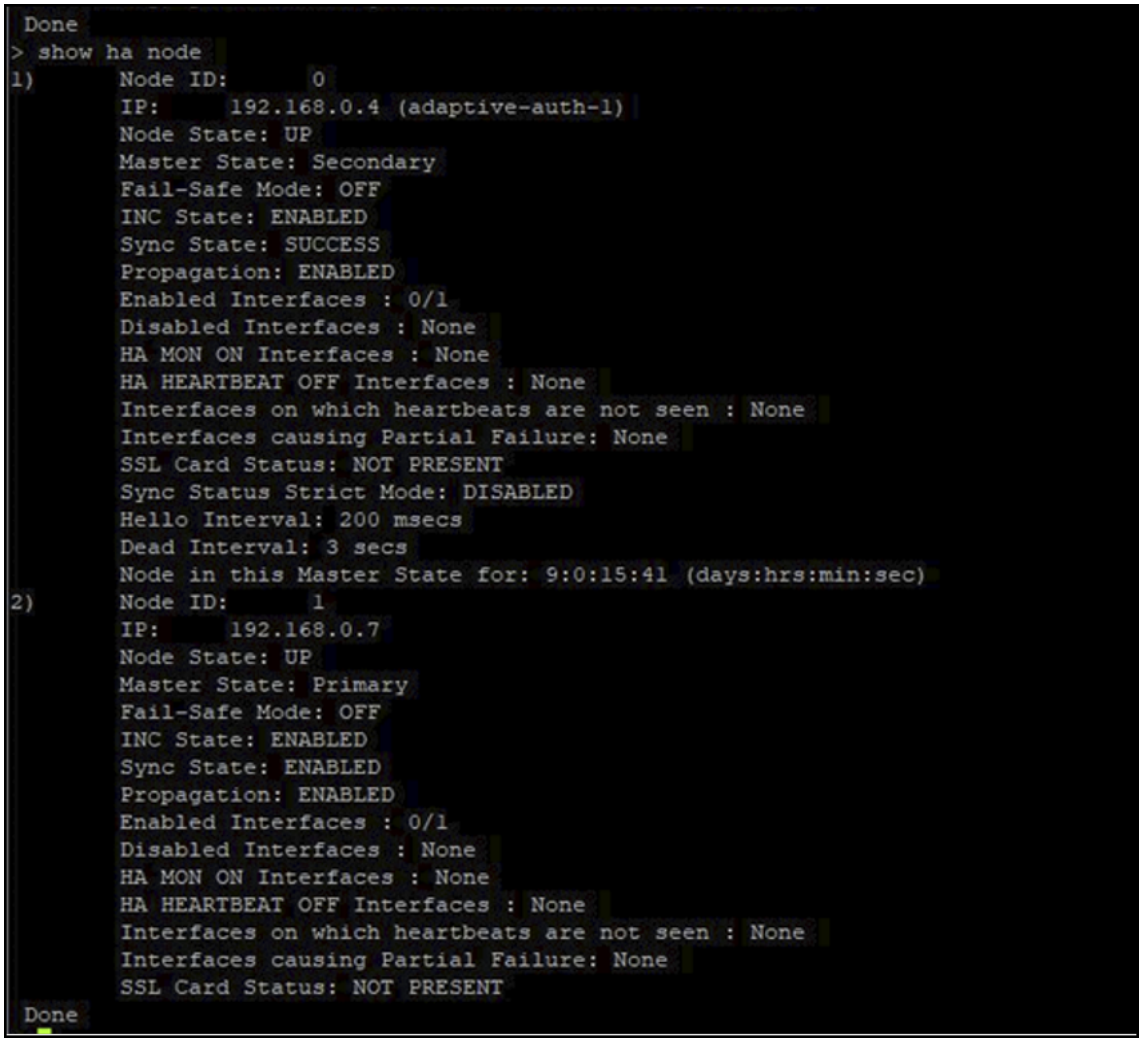
> **Important**
>
> The encrypted secret and encryption parameters for the OAuth profile are different on the Adaptive Authentication primary vs secondary HA gateways. Make sure you obtain the encrypted secret from the primary HA gateway and also run these commands on the primary HA gateway.

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:

Workspace platform

- Custom domain is not supported when you access Citrix Workspace through Web extensions, except on Safari.
- Currently supports only one custom domain per customer.
- A custom domain can only be linked to the default Workspace URL. Other Workspace URLs added through the multi-URL feature can't have a custom domain.
- If you have a custom domain configured on the previous solution and are using SAML or Azure AD to authenticate Citrix Workspace access, you're **unable** to configure a custom domain on the new solution without **deleting your existing** custom domain first.

Citrix Workspace app for Windows

- This feature is not supported on Citrix Workspace app for Windows version 2305 and 2307. Update to the latest supported version.

Configure multiple Workspace URLs

February 22, 2024

Overview

You can now create multiple Workspace URLs (subdomains of cloud.com) and use these URLs as policy inputs. For example, you might want different branding, authentication methods, and resources for different divisions within your organization. With the multiple Workspace URLs feature, you can now have a separate branding, authentication methods, and resources for each of your URLs.

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

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

- Different branding of the UI (post login)
- Different sets of apps and desktops
- Different authentication configuration

Select unique Workspace URLs

The workspace URL that you select must be unique. Citrix Cloud rejects Workspace URLs that are already in use by other customers. It's recommended to use a naming convention that contains a string that is unique to your organization.

> **Note:**
>
> Avoid using generic URLs such as `workspace.cloud.com`or `mystore.cloud.com`.

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

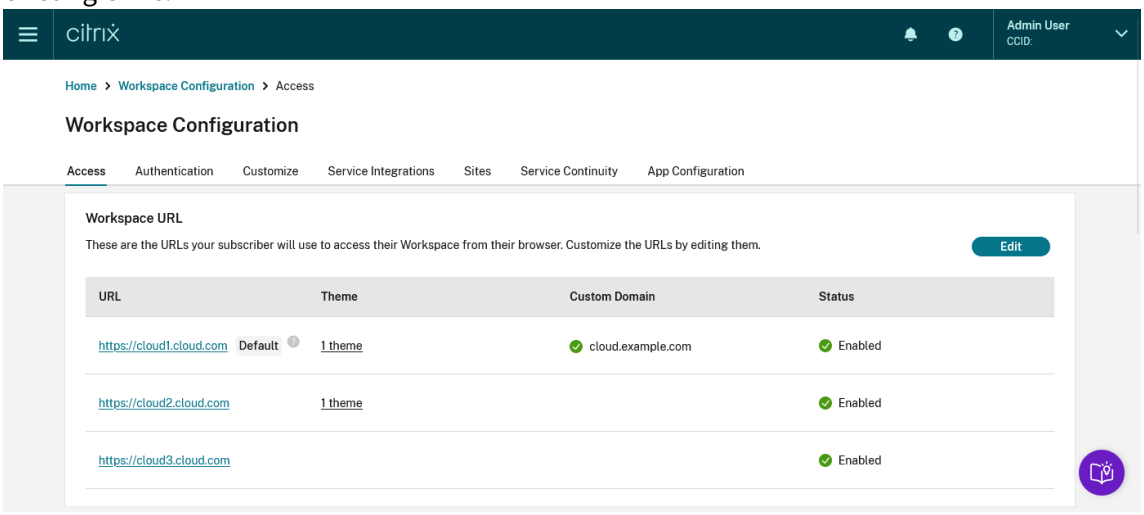
- `YourOrgsales.cloud.com`
- `YourOrgengineering.cloud.com`
- `YourOrgmarketing.cloud.com`

Add multiple Workspace URLs

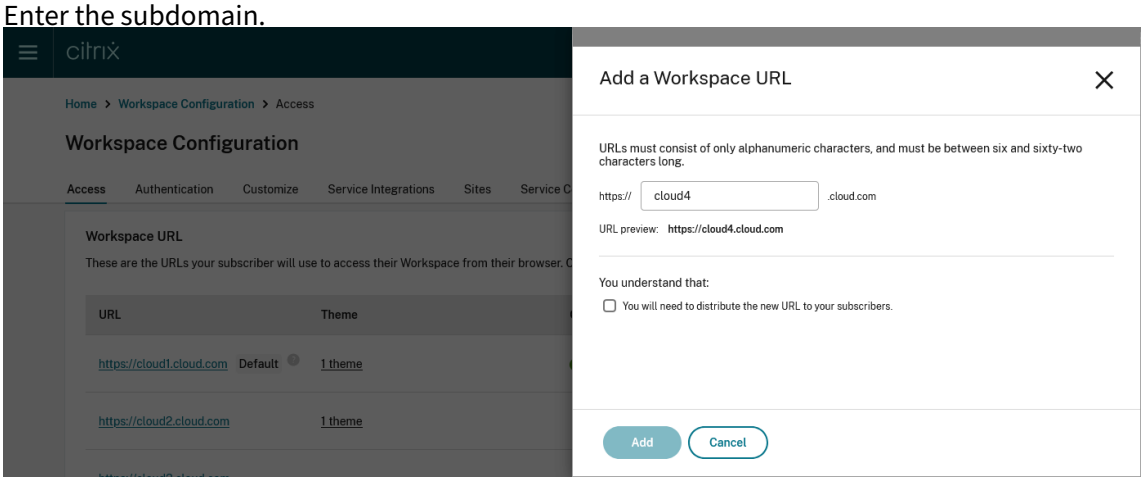
You can add multiple URLs from the Citrix Cloud console as follows.

1. Go to Citrix Cloud and sign in with your credentials.

2. Navigate to **Workspace Configuration** > **Access**. Under **Workspace URL**, you can find a list of existing URLs.



3. To add URL, click **Edit** > **Add Workspace URL**.
4. Enter the subdomain.



5. Click **Add** to save the URL. You must select the checkbox as an acknowledgment that you must provide the new URLs to your end users post configuration.

Add multiple URLs using PowerShell

You can also use the PowerShell script to add multiple Workspace URLs. You need a client ID and Secret. For more information, see Citrix Cloud API.

1. Download a copy of the Store configuration PowerShell module, and unzip it.
2. Unpack the .zip to your current user's desktop and place it inside a folder called **StoreConfig**.

Sample script to configure multiple workspace URLs

Use the following script to ensure that the connection to configure Workspace is made using TLS version 1.2:

```
[System.Net.ServicePointManager]::SecurityProtocol = [System.Net.
    SecurityProtocolType]::Tls12;
<!--NeedCopy-->
```

View the PowerShell help for each cmdlet using these commands (optional) The PowerShell cmdlet `Get-Help` gives detailed instructions for the Get and Set-WorkspaceCustomConfiguration cmdlets.

```
Get-Help Get-WorkspaceCustomConfiguration -detailed
Get-Help Set-WorkspaceCustomConfiguration -detailed
<!--NeedCopy-->
```

Loading the PowerShell module

```
$ModulePath = "$env:UserProfile\desktop\StoreConfig\Citrix.Workspace.
    StoreConfigs.psm1")

if (Test-Path -Path $ModulePath)
{

    Write-Host "Importing StoreConfig PowerShell Module..." -
        ForegroundColor "Green"
    Import-Module -Name $ModulePath -verbose
 }

else
{

    throw "StoreConfig PowerShell Module not found."
 }


[string]$APIClientID = "<insert ClientID>"
[string]$APIClientSecret = "<insert ClientSecret>"
<!--NeedCopy-->
```

Existing Workspace URL Set a variable to the value of existing URL for the workspace.

```
$WSPURL = "wspmultiurlmain.cloud.com"
<!--NeedCopy-->
```

Specify new URLs Specify the new URLs that you want to create in a list, including any existing URLs.


```
$WorkspaceHosts = @($WSPURL,"wspmultiurl2.cloud.com","wspmultiurl3.
    cloud.com")
<!--NeedCopy-->
```

Performing the URL update Run the cmdlet `Set-WorkspaceCustomConfigurations` with the `$WorkspaceHosts` list as the argument to the `-WorkspaceHosts` parameter to update the URL list for the workspace. Give the existing URL as the argument to the `-WorkspaceUrl` parameter.

```
Set-WorkspaceCustomConfigurations -WorkspaceUrl $WSPURL `
                                  -WorkspaceHosts $WorkspaceHosts `
                                  -ClientId $APIClientID `
                                  -ClientSecret $APIClientSecret `
                                  -Verbose

<!--NeedCopy-->
```

Check the Store configuration for your customer

```
Get-WorkspaceCustomConfigurations -WorkspaceUrl $WSPURL `
                                  -ClientId APIClientID `
                                  -ClientSecret $APIClientSecret `
                                  -Verbose
<!--NeedCopy-->
```

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

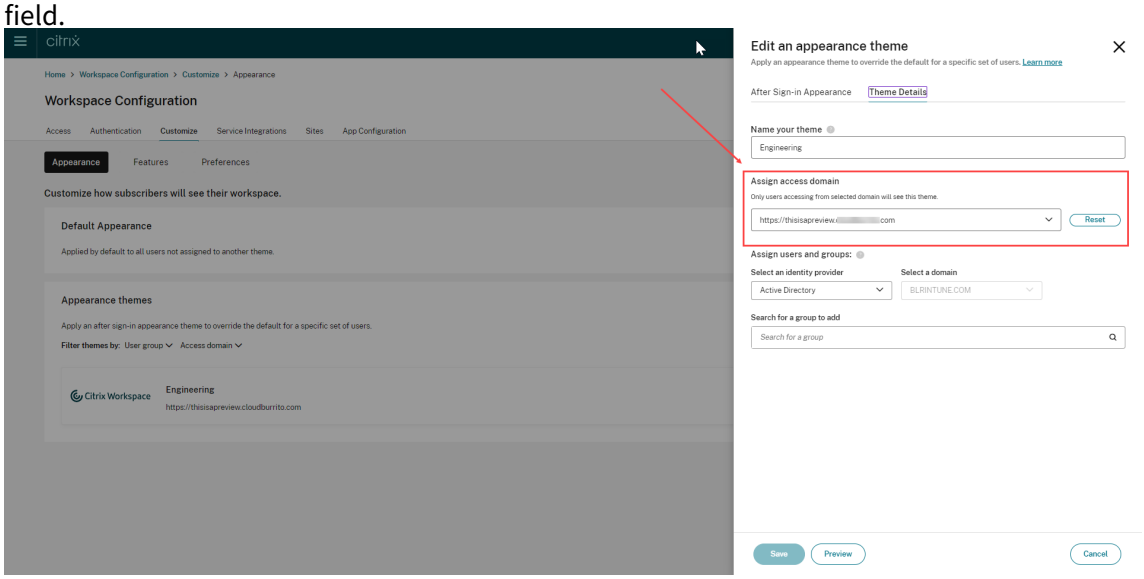
Configure themes and logos based on Workspace URLs

With the multiple URL feature, you can create and assign separate Appearance themes and logos for each of the URLs. It enables you to vary the theme and logo that is visible to end users, based on the Workspace URL.

To create themes and logos based on URLs:
Sign in to the Citrix Cloud Console portal.

1. Navigate to **Workspace Configuration > Customize > Appearance**.
2. Select **Add theme** or modify an existing theme using the edit option.
3. On the **AfterSign-in Appearance** tab, upload the logo and select the theme colors.

4. On the **Theme Details** tab, enter the required Workspace URL in the **Assign access domain** field.



5. Save your theme configuration. For more information on creating a theme, see Create multiple custom themes.

Application of themes

Themes can be configured and applied for the following use cases:

- **Apply theme to a specific URL:** The configured theme applies to any end user using te particular Workspace URL. The user group membership isn't considered as a factor in these cases.
- **Apply the theme to one or more user groups:** The theme applies to end users who belong to any of the selected user groups. In this case, the theme is applied regardless of the URL used.
- **Apply theme to a specific URL and one or more user groups:** The theme applies to an end user if they belong to any of the selected user groups and are using the particular URL.

The theme prioritization mechanism is the same as before. For more information, see Prioritize custom themes

In case no theme has been configured, the default theme is applied. It's also applied in the following scenarios:

- When viewing any pre-login messages or UI
- When viewing the sign-in screen, unless a third-party provider is used which has its own sign-in page
- After sign-in, if no appearance theme is configured for the URL

Filter resources based on Workspace URLs

With the new multiple Workspace URL feature, you can filter and deliver resources based on the Workspace URL that the end users are using.
There are two methods to filter resources based on Workspace URLs:

- Using Secure Private Access(SPA)
- Using DaaS Admin Console (Studio)

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 Workspace URLs. Access Policies can be configured for delivery groups using the Workspace URL filter.

For more information, see Citrix Secure Private Access

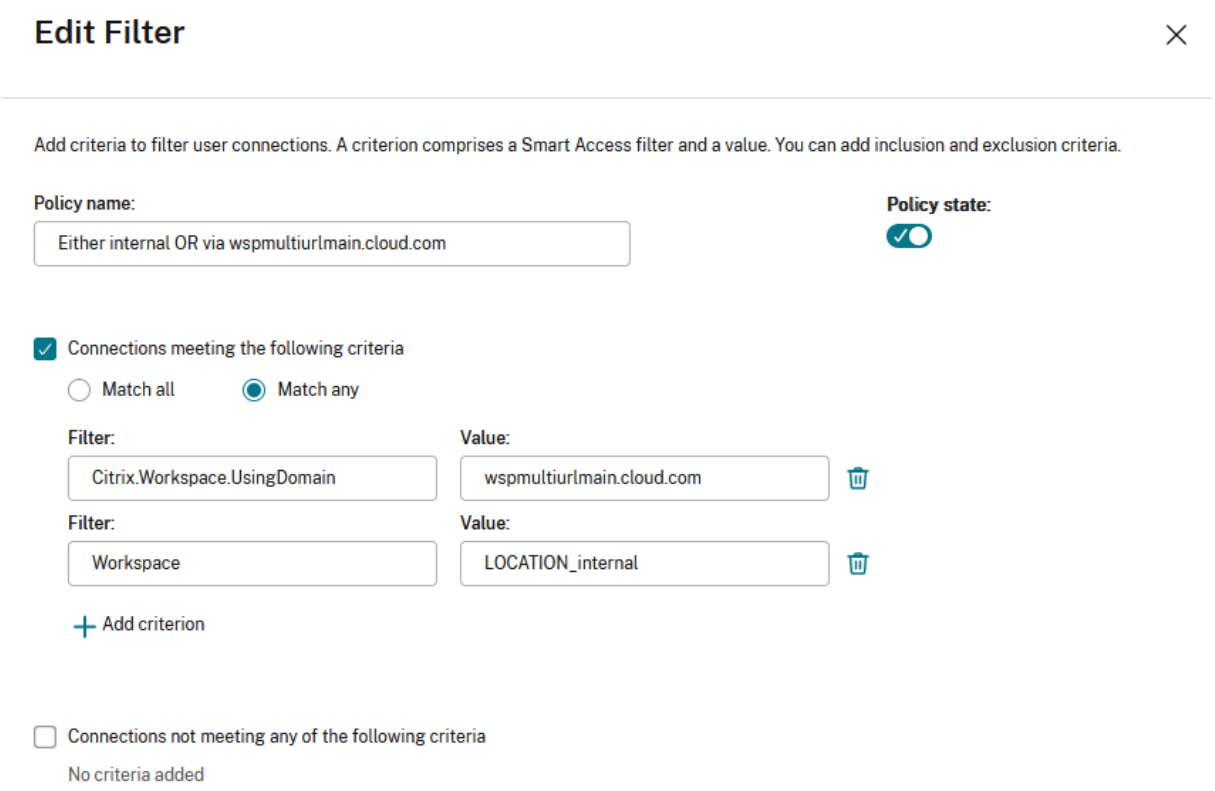
Resource Filtering using DaaS admin console (Studio)

You can now configure Access Policies for delivery groups based on Workspace URLs. You can control end users'access to resources based on the Workspace URL that they're using.
To configure an Access Policy for delivery groups based on Workspace URLs, you need to apply the following SmartAccess filters. The filter values are also sent as SmartAccess tags to the DaaS service. It is applicable in both the scenarios:

- while listing apps and desktops published by DaaS
- while launching an app or desktop

Filter	Value	Description
Citrix.Workspace.UsingDomain	example.cloud.com	Allows filtering of delivery group resources by Workspace URL. The value is the fully qualified domain name of the Workspace URL.
Citrix-Via-Workspace	True	Indicates that the end user is using the Workspace service, rather than an on-premises StoreFront deployment.

> **Note:**
>
> The SmartAccess tags are sent automatically. DaaS treats requests from Workspace as being not through Citrix Gateway. If you are not using Network Location or Device Posture, you need to add filter criteria for these filters to the **Non-Citrix Gateway Connections** rule.



This allows filtering of apps and desktops within a delivery group, based on the following criteria:

- the workspace URL that is being used by the end users
- whether users have signed into Workspace or StoreFront

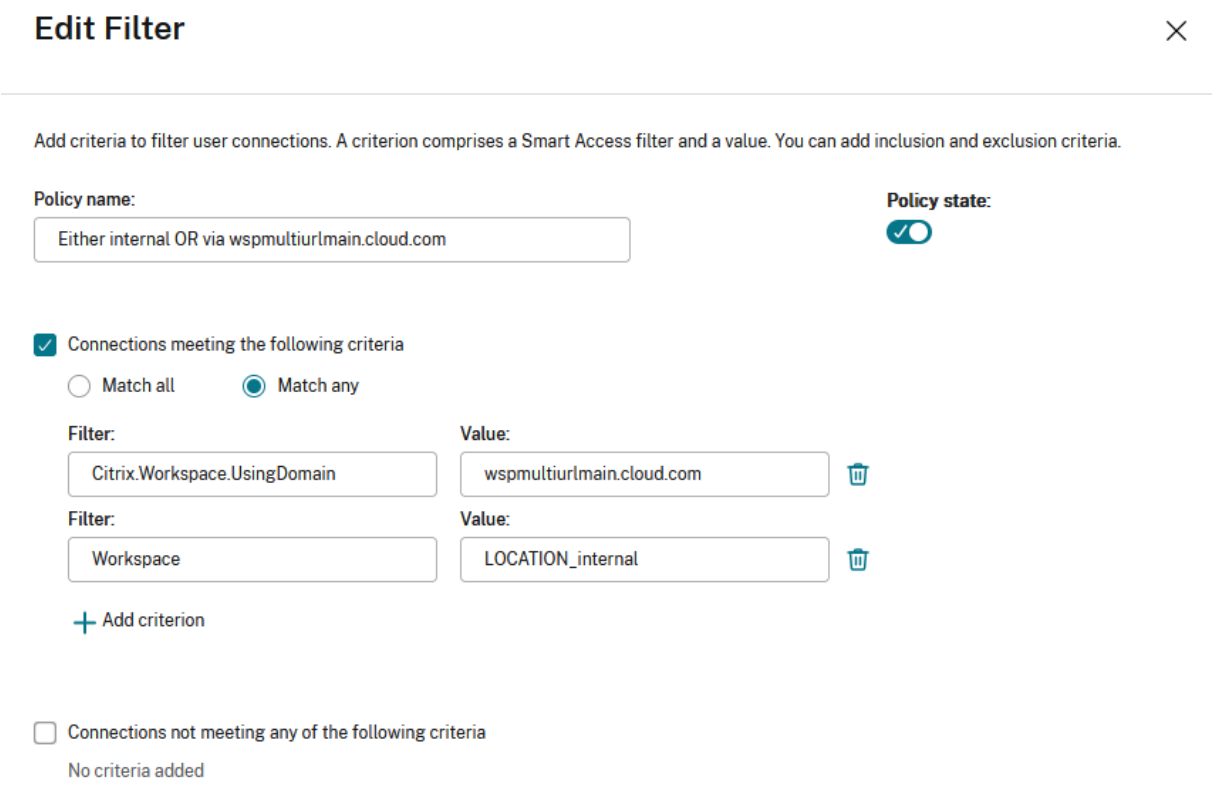
For more information on configuring an access policy for a delivery group, see Manage delivery groups.

> **Note:**
>
> Enabling the adaptive access (Network Location or Device Posture) features causes DaaS to treat requests via Workspace as via Gateway. If either feature is switched on, the multiple URL filter criteria need to be added to the Citrix Gateway Connections rule instead. These features cause other SmartAccess tags to be sent. For more information, see Adaptive Access based on user's network location and Device Posture.

Create an access policy rule for multiple URL workflows

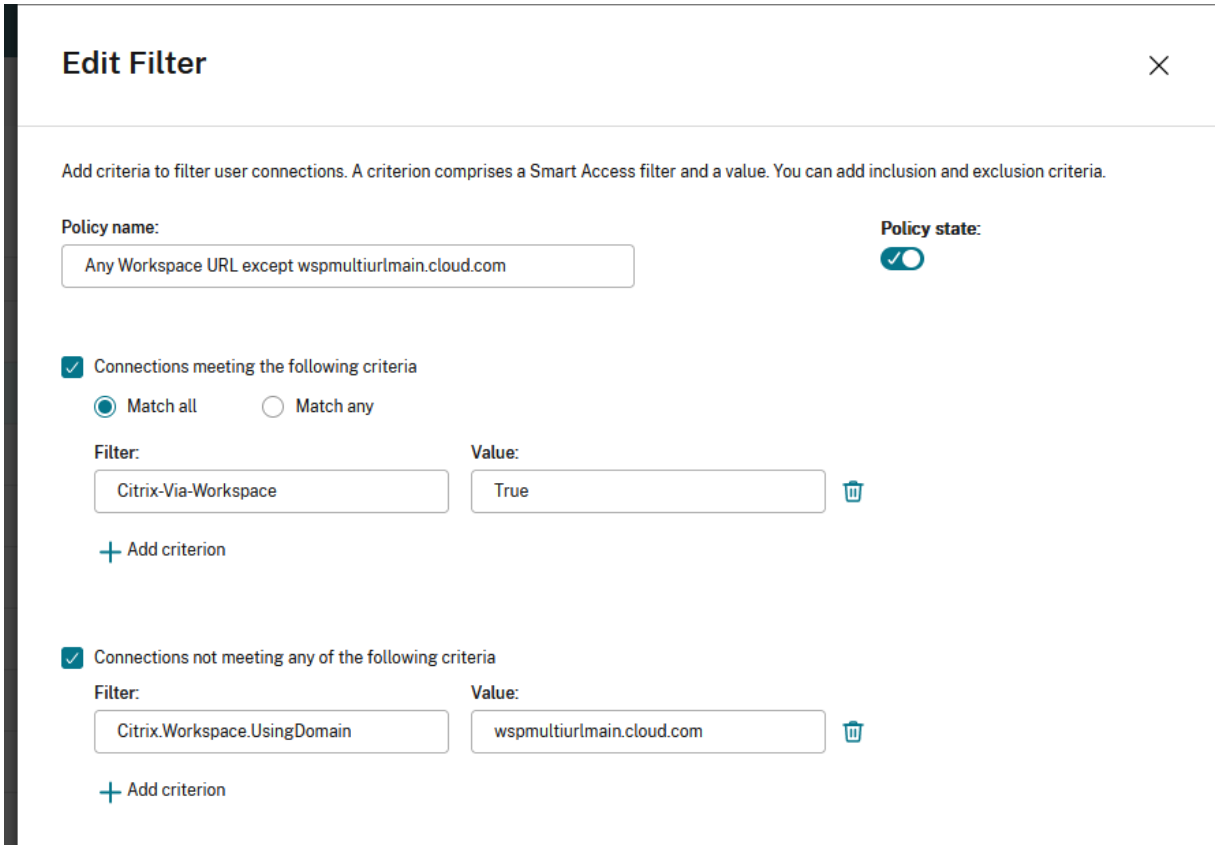
1. To create an access policy rule, go to **Edit Delivery Group > Access Policy**, and click Add. Access policies can only be changed once a delivery group has been created.
2. Add a descriptive policy name.
3. Select one of the following criteria for your filters:
    - **Match any**: The access policy allows access if any of the given filter criteria matches the incoming request.
    - **Match all**: The access policy allows access only if all of the given filter criteria match the incoming request.
4. Add values for the `**Citrix.Workspace.UsingDomain**` and `**Citrix-Via-Workspace**` filters.

For example, in the following scenario the use of **Match any** filter means that this rule allows access from either a user using , or a user connecting from an internal network (as per the Network Location configuration). For more information, see [Adaptive access based on user's network location](/en-us/citrix-daas/manage-deployment/adaptive-access/adaptive-access-based-on-users-network-location.html).

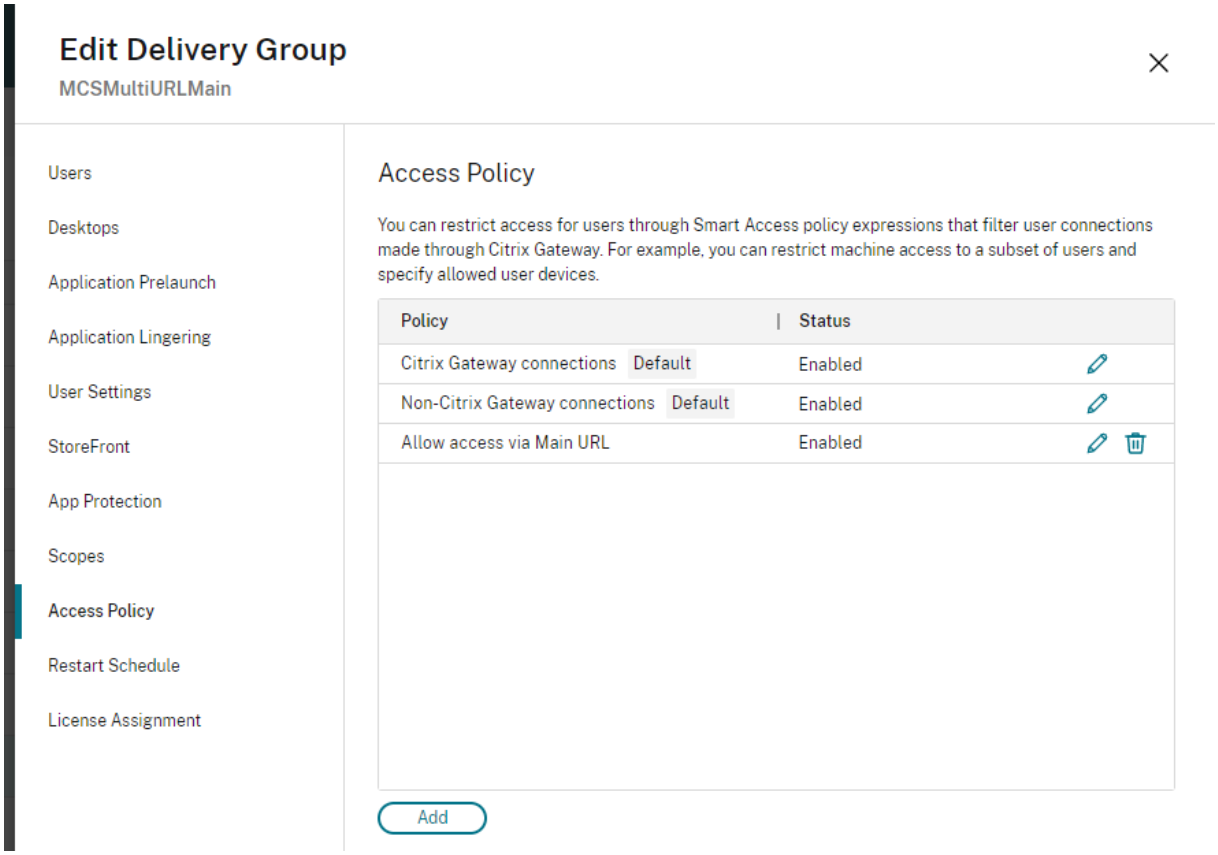


Changing the filter to **Match all** would mean that the rule only allows access to a user using

<wspmultiurlmain.cloud.com> from an internal network.



Once you confirm the changes, the new policy appears on the Access Policy page. For more information, see Manage Delivery Groups



Configure nFactor authentication flows based on Workspace URLs

You can associate authentication policies with a Workspace URL using the Adaptive Authentication service. This enables you to configure different authentication policies for the end users based on the Workspace URL they're using.

You can create a policy or edit an existing one to associate it with a Workspace URL. Use one of the following methods:

- Configure multiple authentication policies using UI
- Configure multiple authentication policies using the Command Line interface

Configure multiple authentication policies using the UI

The Adaptive Authentication service lets you create policies that authenticate your end users based on the Workspace URL that they're using.

Step 1: Configure a series of authentication actions and policies that you want to use for the Workspace 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

Policy syntax

Check for a particular Workspace URL using exact string matching.

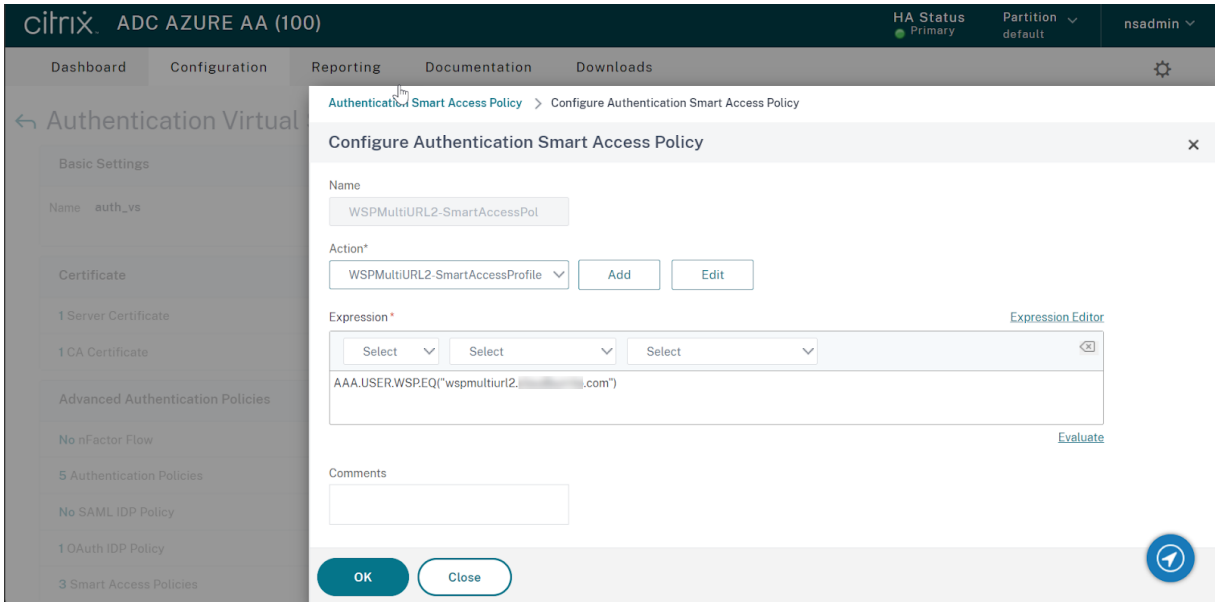
```
AAA.USER.WSP.EQ("wspmultiurlmain.cloud.com")

<!--NeedCopy-->
```

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

```
AAA.USER.WSP.CONTAINS("wspmultiurlmain")
<!--NeedCopy-->
```

Step 2: Configure an authentication policy and add your Workspace URL as the expression. The authentication policy is then valid for the Workspace 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.

Send *SmartAccess* tags to DaaS based on Workspace URL

DaaS delivery groups support SmartAccess tags based on the Workspace URL used. The tags can be a fixed set as explained in Configure Workspace to filter DaaS resources based on Workspace URL or you can use the **Citrix.Workspace.UsingDomain** filter or any other *SmartAccess* tag you want to use to influence DaaS resource enumeration behavior. The AAA admin can define multiple conditions that control when *SmartAccess* tags are sent to DaaS delivery groups.

1. Configure a *SmartAccess* tag profile with a tag string that you want to send to DaaS.
2. Configure a *SmartAccess* tag policy expression and link the policy to the action you created earlier.
3. Now bind the authentication policies to your AAA virtual server.

Configure multiple authentication policies using the Command Line Interface

Send a *SmartAccess* tag based on the Workspace URL used

Create the *SmartAccess* Tag profiles

```
add authentication smartAccessProfile WSPMultiURLMain-
    SmartAccessProfile -tags "WSPMultiURLMain"

add authentication smartAccessProfile WSPMultiURL2-SmartAccessProfile -
    tags "WSPMultiURL2"

add authentication smartAccessProfile WSPMultiURL3-SmartAccessProfile -
    tags "WSPMultiURL3"

<!--NeedCopy-->
```

Create the *Smart Access* Tag policies

```
add authentication smartAccessPolicy WSPMultiURLMain-SmartAccessPol -
    rule "AAA.USER.WSP.EQ(\"wspmultiurlmain.cloud.com\")" -action
    WSPMultiURLMain-SmartAccessProfile

add authentication smartAccessPolicy WSPMultiURL2-SmartAccessPol -rule
    "AAA.USER.WSP.EQ(\"wspmultiurl2.cloud.com\")" -action WSPMultiURL2-
    SmartAccessProfile

add authentication smartAccessPolicy WSPMultiURL3-SmartAccessPol -rule
    "AAA.USER.WSP.EQ(\"wspmultiurl3.cloud.com\")" -action WSPMultiURL3-
    SmartAccessProfile
<!--NeedCopy-->
```

Show *Smart Access* Profiles and Policies

```
show authentication smartAccessProfile
show authentication smartAccessPolicy
```



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

Bind the Policies to the Adaptive Authentication virtual server called “auth_vs”

```
bind authentication vserver auth_vs -policy WSPMultiURLMain-
    SmartAccessPol -priority 10

bind authentication vserver auth_vs -policy WSPMultiURL2-SmartAccessPol
     -priority 20

bind authentication vserver auth_vs -policy WSPMultiURL3-SmartAccessPol
     -priority 30

<!--NeedCopy-->
```

Email Discovery to add Workspace URLs to Citrix Workspace app

Email discovery adds all the Workspace URLs configured in the list of service URLs as stores. If you want to add two or more stores through email discovery, configure each Workspace 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.

Workspace Platform

- You can’t disable individual URLs. If you disable a Workspace URL within the Citrix Cloud admin console, it disables all the configured URLs.

Citrix Virtual Apps and Desktops

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

Custom Workspace Domain The workspace is limited to a single custom domain. It's always linked to the Workspace URL marked as Default in the admin console.

Citrix Workspace app To add multiple URLs from the same customer as stores, users must be on the following versions of the Citrix Workspace app clients:

- 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 Workspace 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 Workspace URLs, then only one Workspace 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
}


<!--NeedCopy-->
```

Secure workspaces

February 16, 2024

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

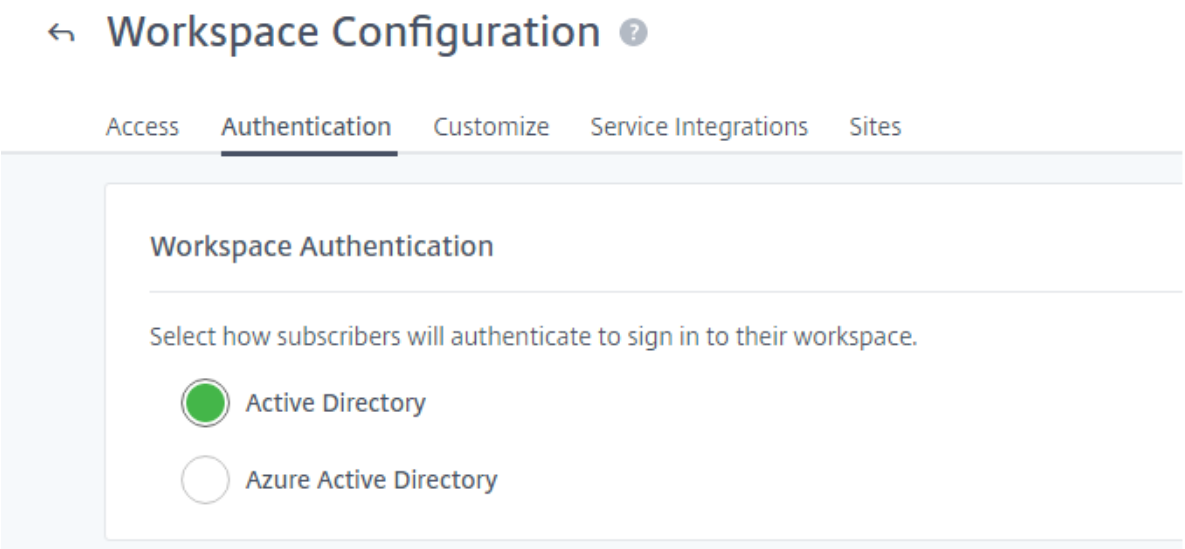
- Active Directory (AD)
- Active Directory plus token
- Azure Active Directory (AAD)
- Citrix Gateway
- Google
- Okta
- SAML 2.0

These authentication options are available to any Citrix Cloud service. For more information, see Tech Brief: Workspace Identity.

Citrix Workspace also supports using Citrix Federated Authentication Service (FAS) to provide single sign-on (SSO) to Citrix DaaS. SSO with FAS removes the need for subscribers to authenticate to DaaS after already signing in to their workspaces using a federated authentication method. For more information, see Enable single sign-on for workspaces with Citrix Federated Authentication Service.

Choose or change authentication methods

After configuring your identity providers, you choose or change how subscribers authenticate to their workspace in **Workspace Configuration > Authentication > Workspace Authentication**.



> **Important:**
>
> Switching authentication modes can take up to five minutes and causes an outage to your subscribers during that time. Citrix recommends limiting changes to periods of low usage. If you do have subscribers logged on to Citrix Workspace 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 subscriber authentication to workspaces.

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.

Active Directory (AD) plus token

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

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

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

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

First-time enrollment

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

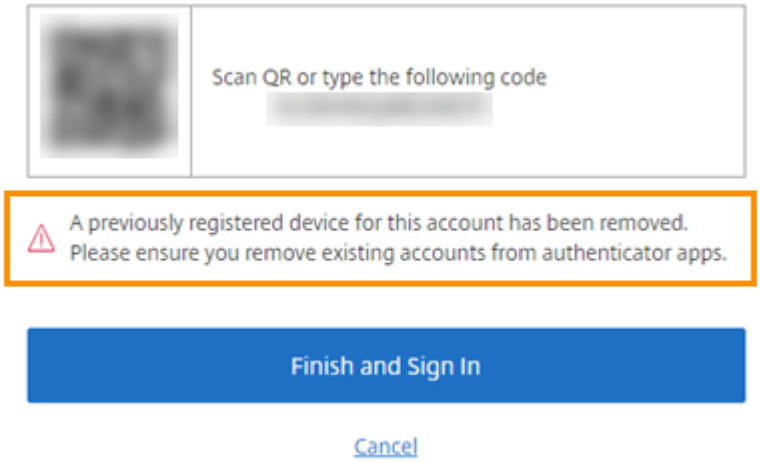
During first-time sign-in to Workspace, subscribers follow the prompts to download the Citrix SSO app. The Citrix SSO app generates a unique one-time password on an enrolled device every 30 seconds.

> **Important:**
>
> During the device enrollment process, subscribers receive an email with a temporary verification code. This temporary code is used only to enroll the subscriber's device. Using this temporary code as a token for signing in to Citrix Workspace 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.

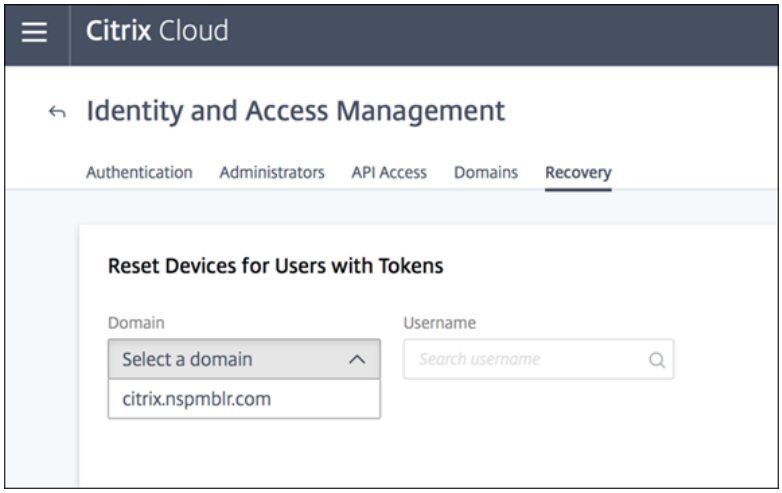
Re-enroll a device

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

- Subscribers can re-enroll their devices using the same enrollment process described in Register devices for two-factor authentication. Because subscribers 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 subscribers by Active Directory name and reset their device. To do that, go to **Identity and Access Management > Recovery**. During the next sign-on to Workspace, the subscriber experiences the first-time enrollment steps.



Azure Active Directory

Use of Azure Active Directory (AD) to manage subscriber authentication to workspaces has the following requirements:

- Azure AD with a user who has global administrator permissions. For more information on the Azure AD 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 Azure AD.
- VDA version 7.15.2000 LTSR CU VDA or 7.18 current release VDA or higher.
- A connection between Azure AD and Citrix Cloud. For information, see Connect Azure Active Directory to Citrix Cloud.

When syncing your Active Directory to Azure AD, the UPN and SID entries must be included in the sync. If these entries aren't synchronized, certain workflows in Citrix Workspace fail.

> **Warning:**
>
> - If you're using Azure AD, don't make the registry change described in CTX225819. Making this change might cause session launch failures for Azure AD 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 Azure AD authentication:

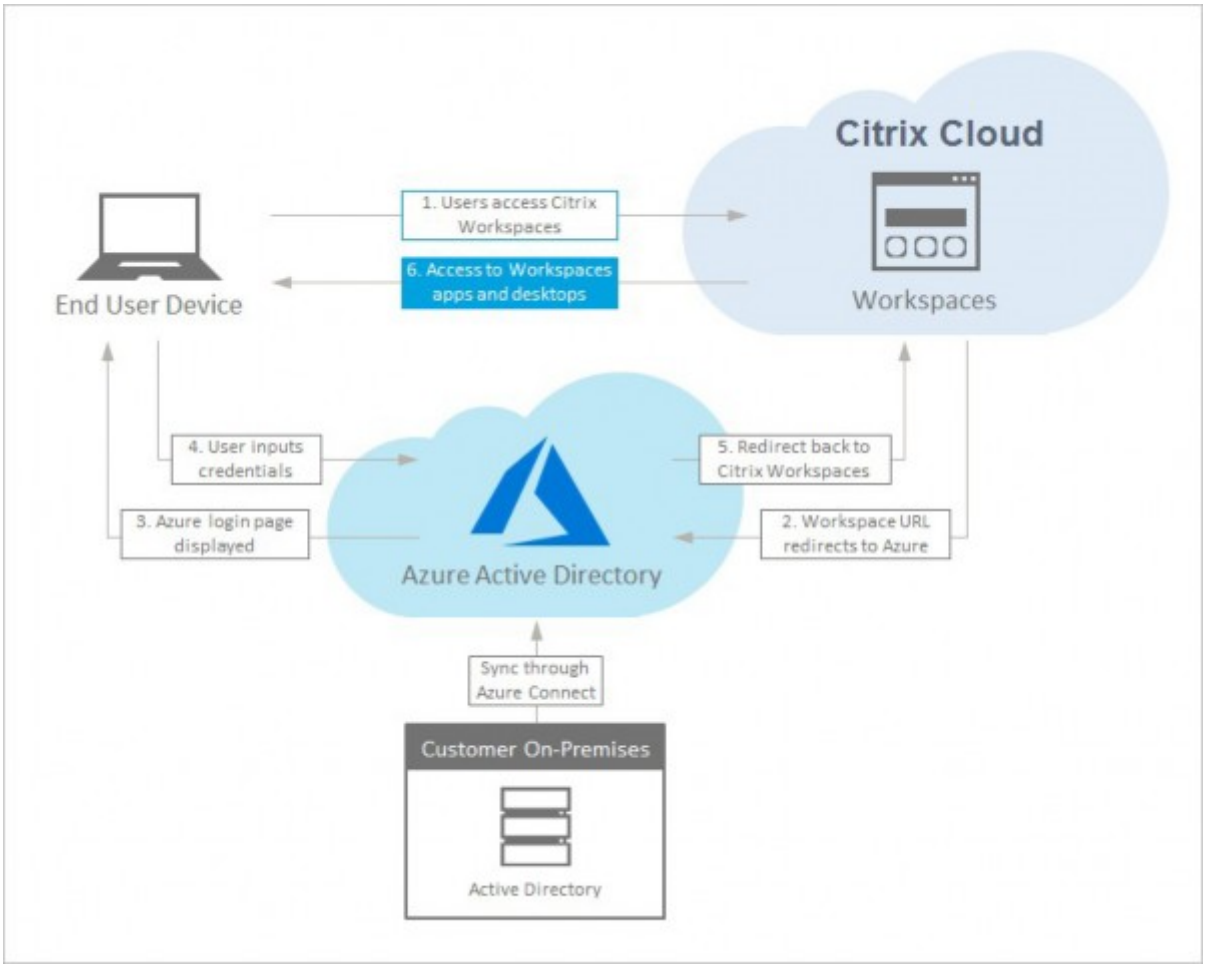
- **Added security:** For security, users are prompted to sign in again when launching an app or a desktop. The password information flows directly from user's device to the VDA that is hosting the session.

- **Sign-in experience:** Azure AD authentication provides federated sign-in, not single sign-on (SSO). Subscribers 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 workspaces with Citrix Federated Authentication Service for more information.

You can customize the sign-in experience for Azure AD. For information, see the Microsoft documentation. Any sign-in customizations (the logo) made in Workspace Configuration do not affect the Azure AD sign-in experience.

The following diagram shows the sequence of Azure AD authentication.



Citrix Gateway

Citrix Workspace supports using an on-premises Citrix Gateway as an identity provider to manage subscriber authentication to workspaces. 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.
- Subscribers must be Active Directory users to sign in to their workspaces.
- 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.

Subscriber experience of Citrix Gateway

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

1. The subscriber navigates to the Workspace URL in their browser or launches Workspace app.
2. The subscriber 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 Workspace sign-in page using the steps described in CTX258331.
3. After successful authentication, the subscriber's workspace appears.

Google

Citrix Workspace supports using Google as an identity provider to manage subscriber authentication to workspaces.

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 Workspace 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.

Subscriber experience with Google

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

1. The subscriber navigates to the Workspace URL in their browser or launches the Workspace app.
2. The subscriber 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 subscriber's workspace appears.

Okta

Citrix Workspace supports using Okta as an identity provider to manage subscriber authentication to workspaces. 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.

Subscriber experience with Okta

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

1. The subscriber navigates to the Workspace URL in their browser or launches the Workspace app.
2. The subscriber 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 subscriber's workspace appears.

Okta authentication provides federated sign-in, not single sign-on (SSO). Subscribers sign in to workspace from an Okta 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 workspaces with Citrix Federated Authentication Service for more information.

SAML 2.0

Citrix Workspace supports using SAML 2.0 to manage subscriber authentication to workspaces. You can use the SAML provider of your choice, provided it supports SAML 2.0.

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 workspaces, see Connect SAML as an identity provider to Citrix Cloud.

Subscriber experience with SAML 2.0

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

Citrix Federated Authentication Service (FAS)

Citrix Workspace supports using Citrix Federated Authentication Service (FAS) for single sign-on (SSO) to Citrix DaaS. Without FAS, subscribers using a federated identity provider are prompted to enter their credentials more than once to access their DaaS.

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

Subscriber sign-out experience

Use **Settings > Log Off** to complete the sign-out process from Workspace and Azure AD. If subscribers close the browser instead of using the **Log Off** option, they might remain signed in to Azure AD.

> **Important:**
>
> If Citrix Workspace times out in the browser due to inactivity, subscribers remain signed in to Azure AD. This prevents a Citrix Workspace timeout from forcing other Azure AD applications to close.

More information

- Tech Brief: Workspace Single Sign-On
- Tech Insights - Citrix Workspace

Integrate services into workspaces

February 22, 2024

This article outlines the steps involved in adding services to Citrix Workspace, 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 **Workspace Configuration** > **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 Workspace.

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

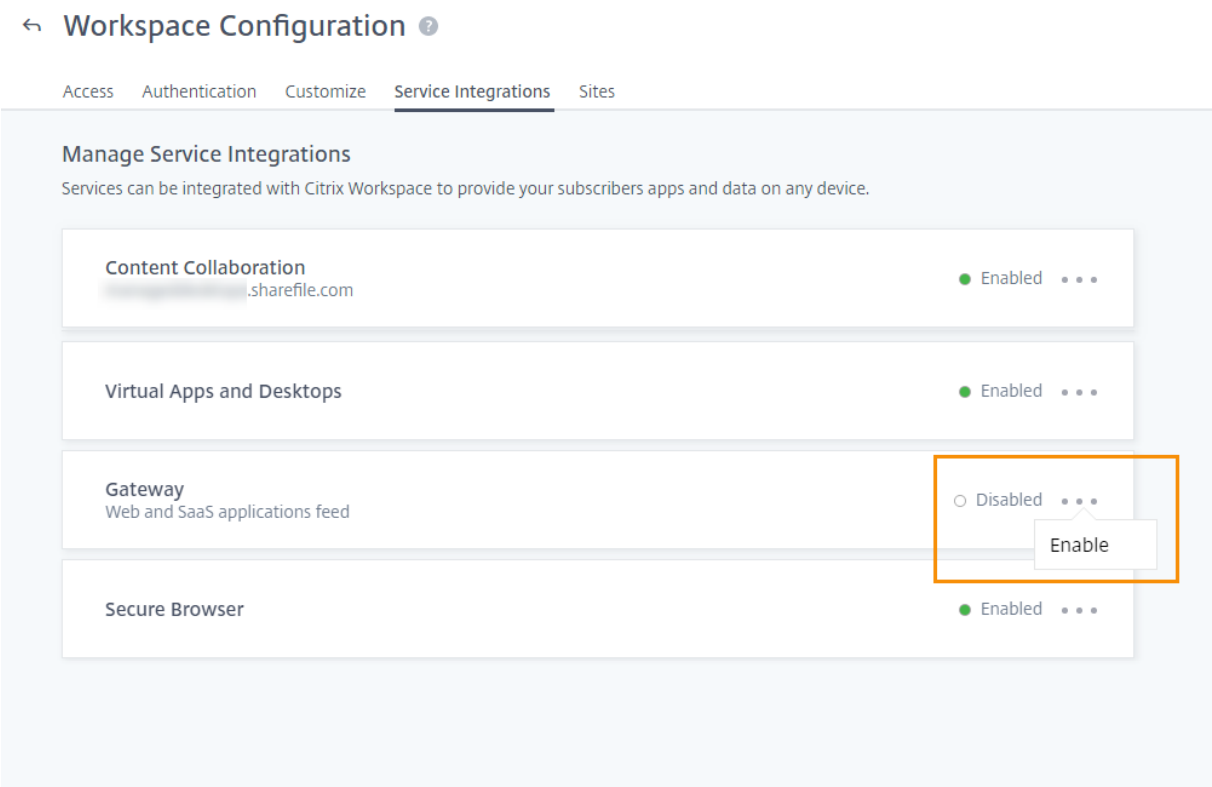
Once you've configured your services, you can integrate them into Citrix Workspace.

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.

> **Note:**
>
> Both the **Citrix Apps Essentials service** and the **Citrix DaaS** display as "Citrix DaaS"in the **Service Integrations** tab of **Workspace Configuration**.

To enable workspace integration for a service:

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

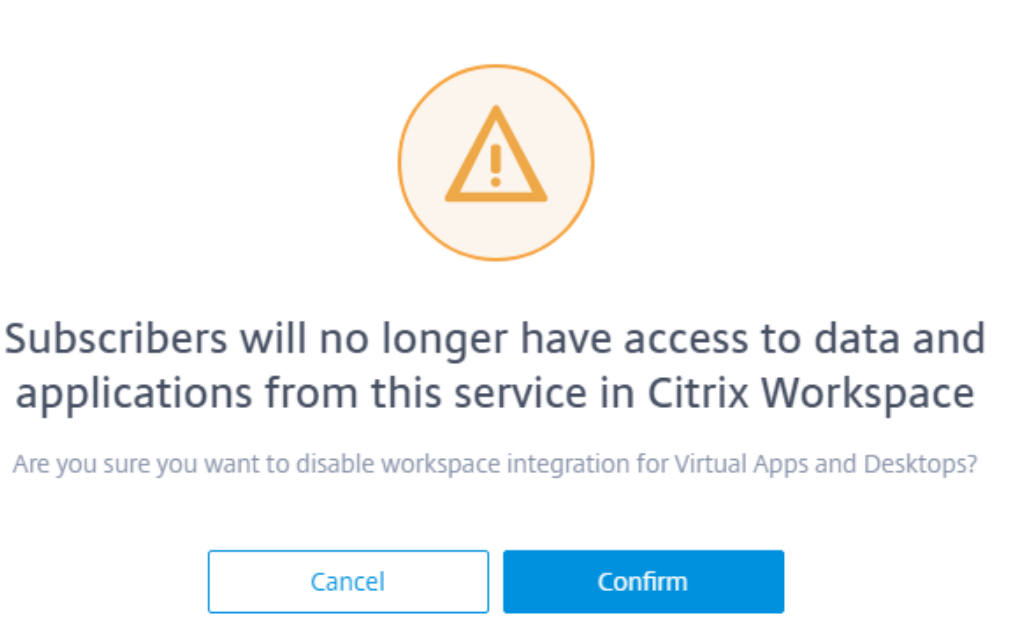


Disable services

Disabling workspace integration blocks subscriber access for that service. This doesn't disable the Workspace URL, but subscribers can't access data and applications from that service in Citrix Workspace.

To disable workspace integration for a service:

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



Configure Citrix Workspace app using Global App Configuration service

March 19, 2024

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 Workspace) 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, Android, iOS, HTML5, and ChromeOS platforms.

Key benefits

The Global App Configuration service lets you perform the following functions from a centralized interface:

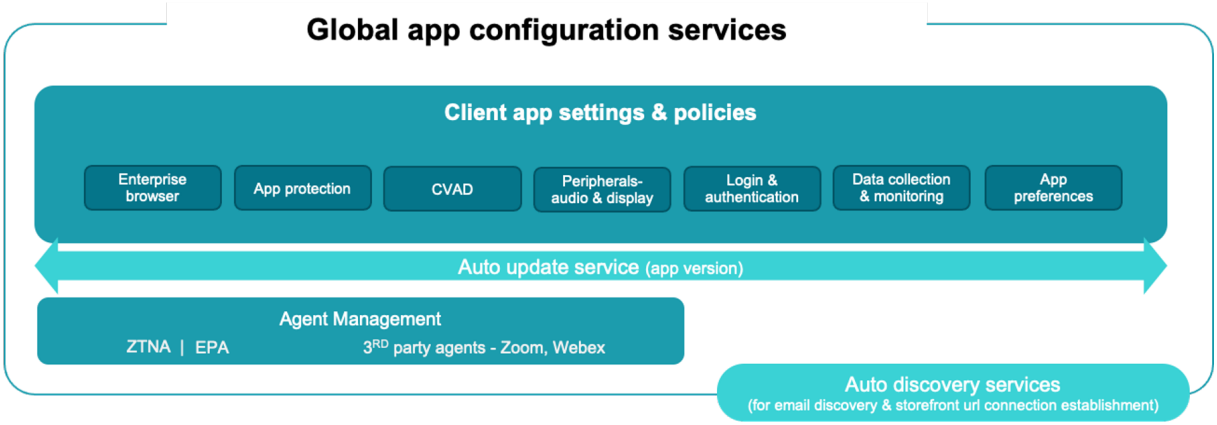
- Configure settings for both managed and unmanaged devices (Bring Your Own Devices)

- 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.



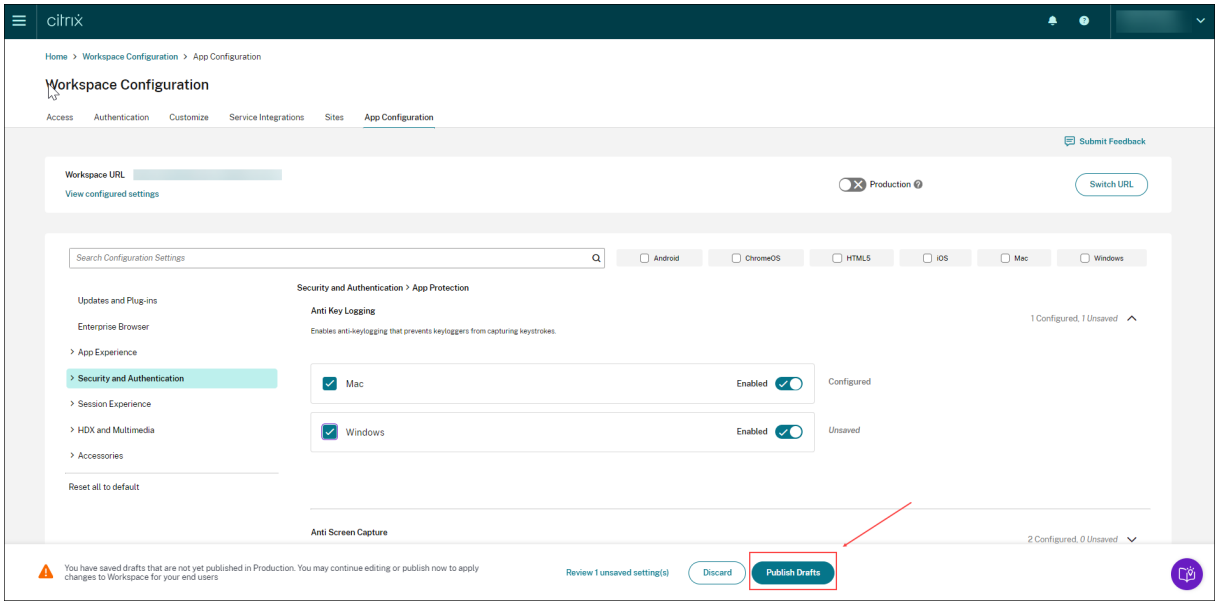
Prerequisites

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
iOS	2104
HTML5	2111
ChromeOS	2203
Android	2104

How to use the Global App Configuration service?

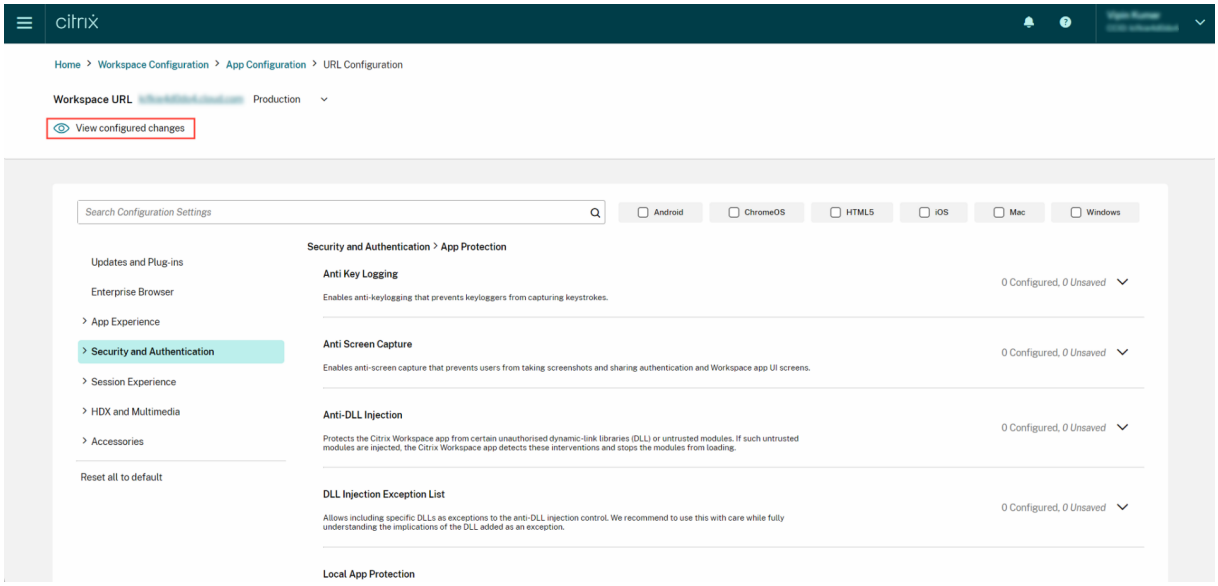
To configure settings, sign in the Citrix Cloud portal and navigate to **Workspace Configuration** > **App configuration**. Modify the app settings as per your organization's policies. You can then click **Publish Drafts** to save and publish your settings.



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

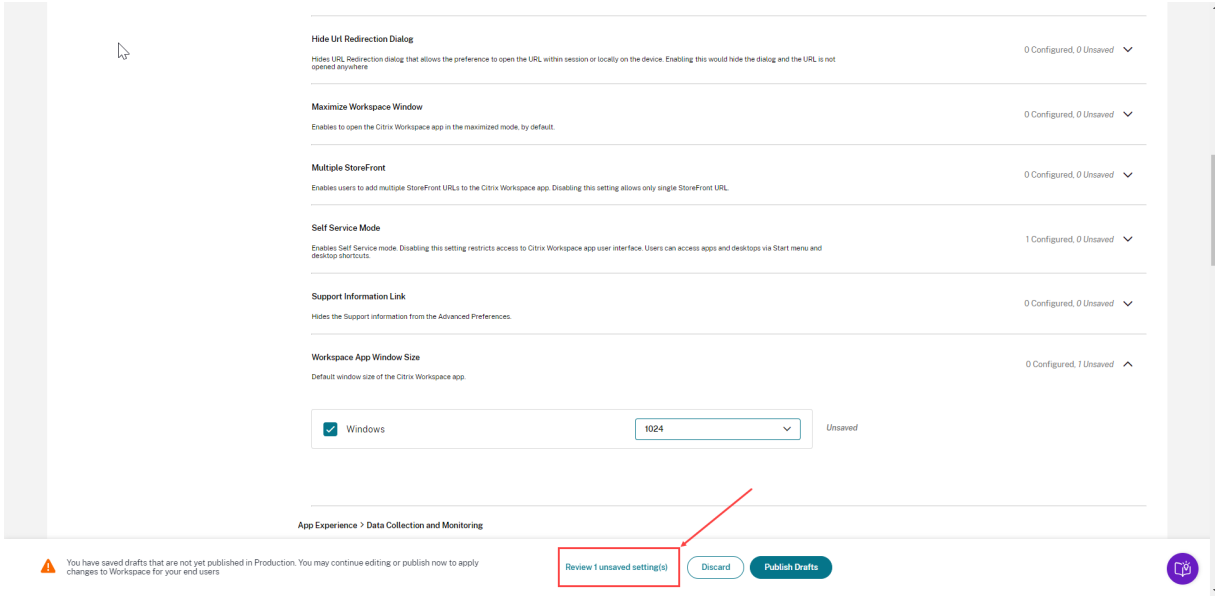
View a summary of configured settings

You can view a summary of the current configuration by clicking the **View configured settings** 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.

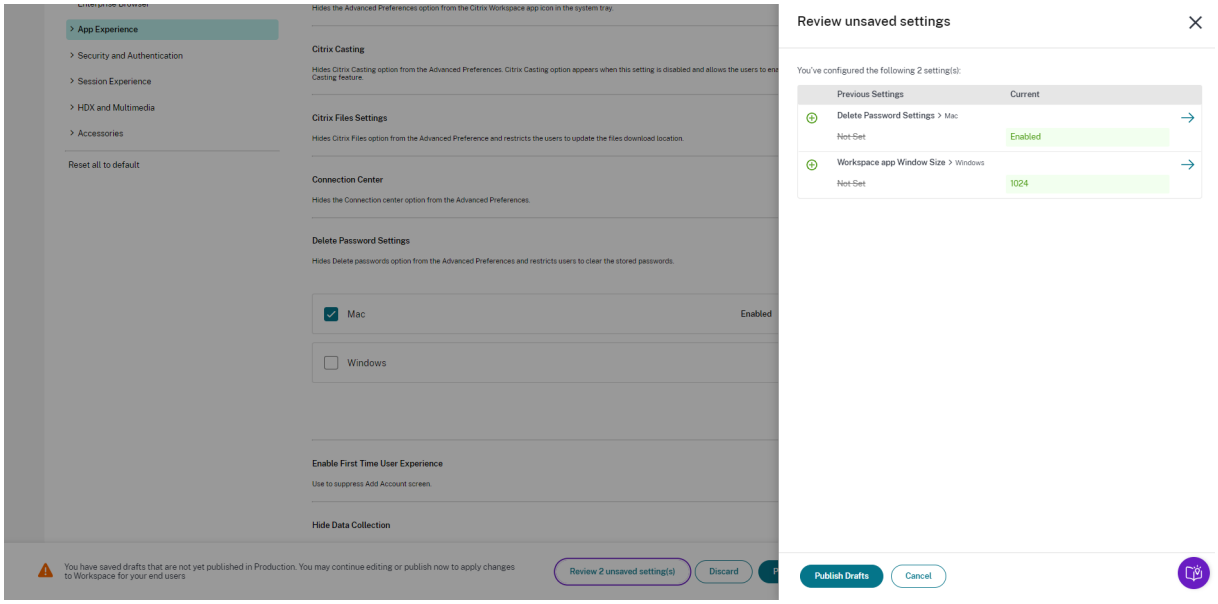


Review unsaved changes

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.



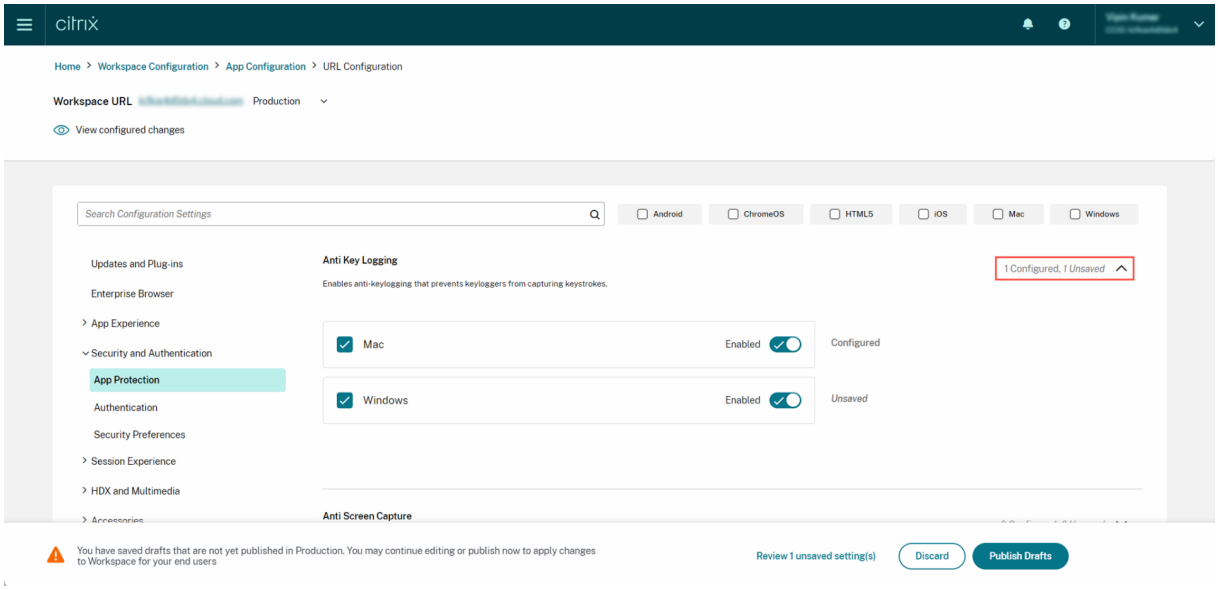
You can also navigate to an unsaved setting by clicking the arrow.



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**

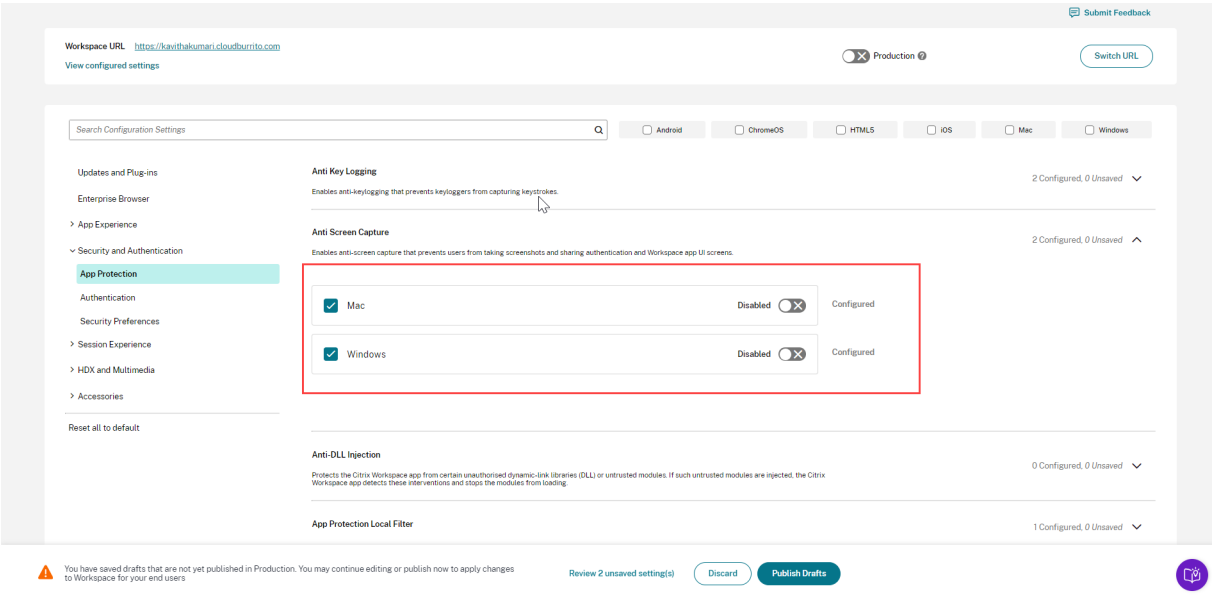
You can locate settings by entering keywords found within the setting's description. It allows for a more flexible search approach, using relevant terms associated with the desired setting.

- **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 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) > Global App Configuration service > Registry**
Citrix Workspace app for Mac	StoreFront and Cloud	**MDM > Global App Configuration service > UserDefaults**
Citrix Workspace app for HTML5	StoreFront	Global App Configuration service > Configuration.js
	Cloud	Global App Configuration service
Citrix Workspace app for ChromeOS	StoreFront	**Google Admin Policy > Global App Configuration service >** Configuration.js

Platform	Store type	Order of precedence
	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

- The Global App Configuration service isn't supported for Linux.
- You can't add more than one Global App Configuration service-enabled store on Windows and Mac.

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

Configure settings for cloud stores

April 18, 2024

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.

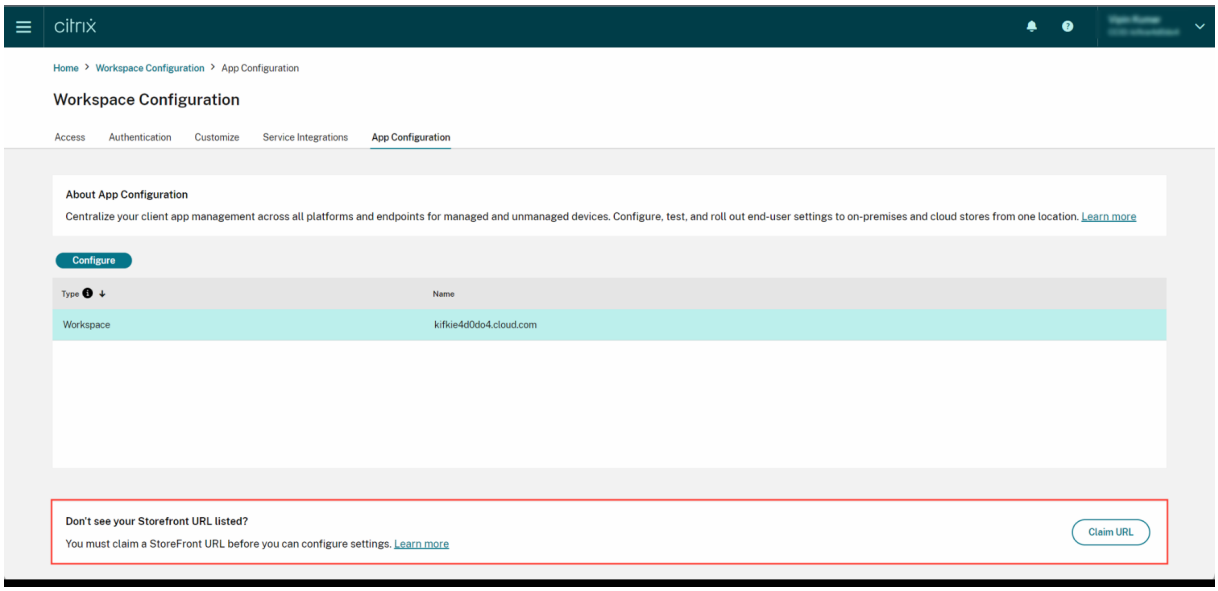
Prerequisites

- 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 services.
- 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 Workspace subscription.

Get started with configuration

You can sign in to your Citrix Cloud account and configure settings from **Workspace Configuration** > **App Configuration**.
Before proceeding, verify if you have the following permissions.

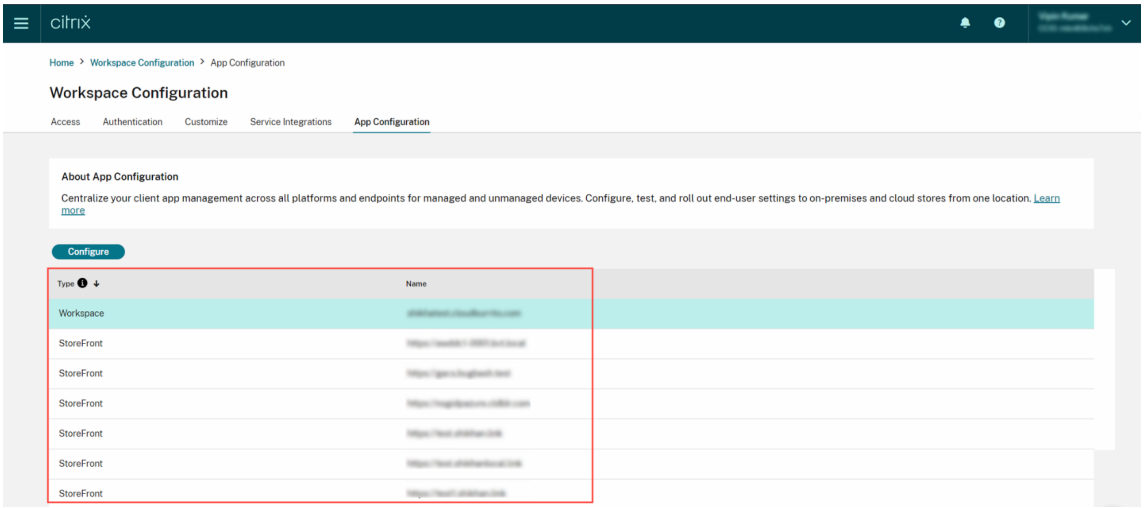
- **Workspace subscription:** The Workspace subscription is required to create a Workspace URL. If you don't have a subscription, you can't add and configure cloud stores. You'll only be presented with an option to configure on-premises stores.
- **Workspace URL:** If you have a Workspace subscription but haven't added your URL yet, you are presented with the following screen. You can click **Claim URL** under the **App Configuration** section to claim your URL.



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. Go to Citrix Cloud and sign in with your Citrix Cloud credentials.
2. Navigate to **Workspace Configuration** > **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.

Setup email based discovery

Email based discovery service allows end users to sign in automatically using their email addresses. They aren't required to furnish their store URLs.
To enable this service for cloud 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 <https://adsui.cloud.com>.
2. Navigate to **Claims** > **Domains** > **Add Domain**.
3. Enter the domain that you want to claim (example, ace.example.com).
4. Click **Confirm**.
5. Copy the DNS token displayed on the screen.
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 have 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

1. Navigate to **Claims** > **Domains**.
2. Go to the domain that you have 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.
5. Click **Save**.

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

Configure settings for on-premises stores

April 18, 2024

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.

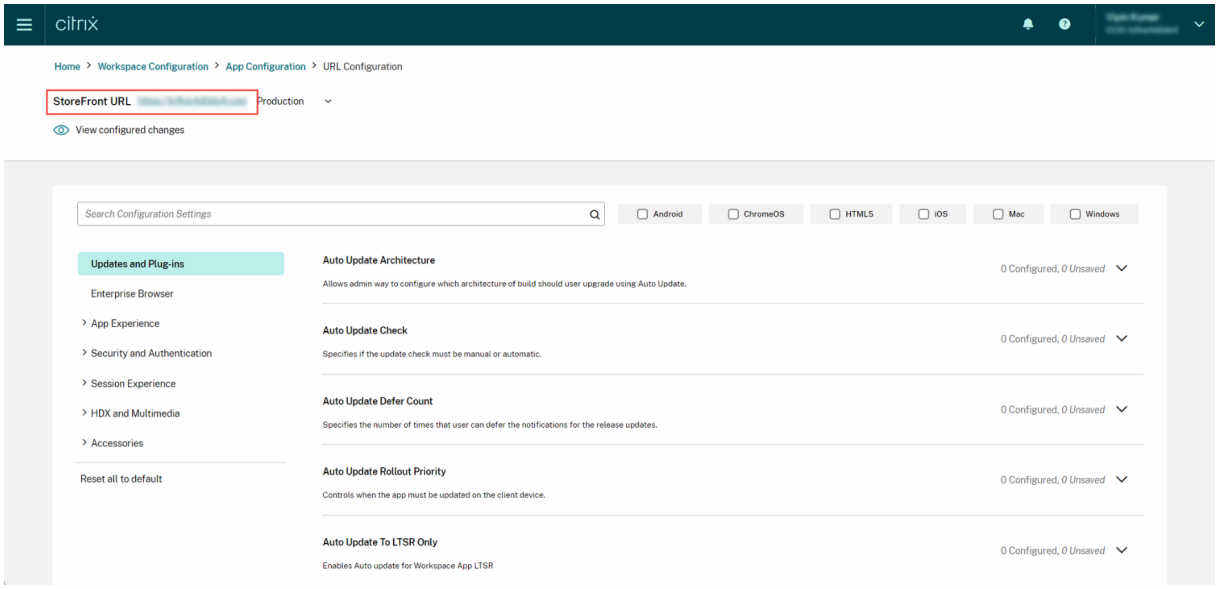
Prerequisites

- 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.

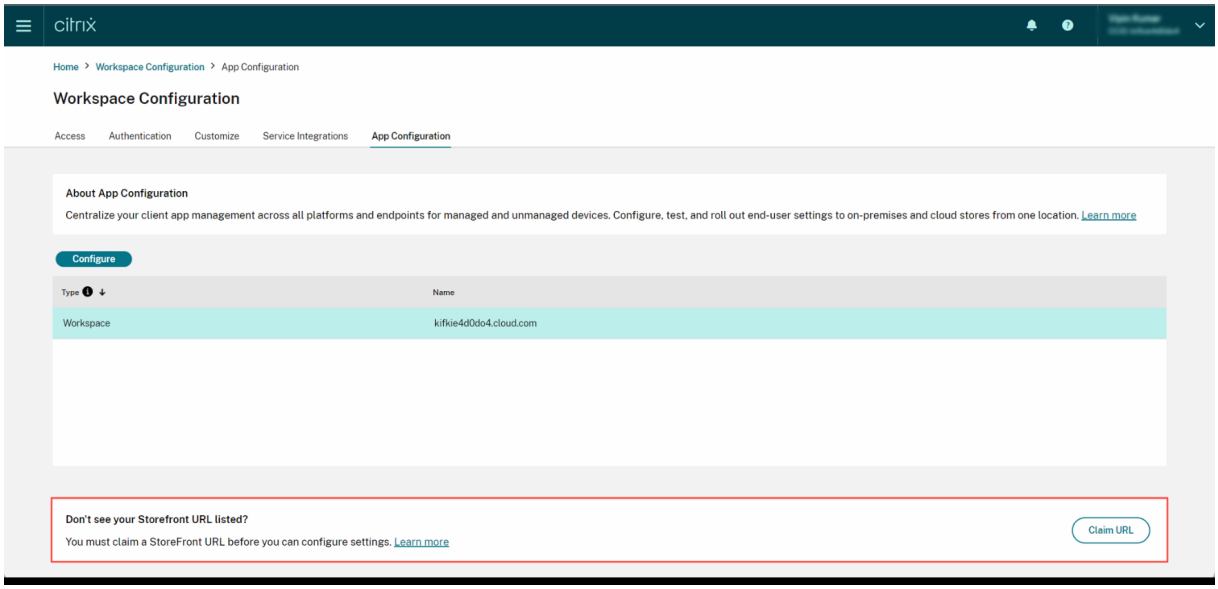
Get started with configuration

To configure settings for an on-premises store, sign in to your Citrix Cloud account and navigate to **Workspace Configuration** > **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 URL** under the **App Configuration** section to claim your URL. For more information, see the Claim a URL for on-premises stores section.



If you have not yet claimed ownership for your StoreFront URL, you are presented with the following screen that prompts you to secure your URL before proceeding. For more information, refer to Claim a URL for on-premises stores.



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. Go to <https://adsui.cloud.com/url> and sign in with your Citrix Cloud credentials.
2. Navigate to **Claims** > **URLs** > **Add URL**.

3. Enter the URL that you want to claim.
4. Click **Confirm**. The verification pop-up appears.

   > **Note:**
   >
   > If the on-premises environment does not have a NetScaler Gateway installed, you won't be able to perform the verification process (from Step 5 onwards). In this case, perform Steps 1 through 4 as described in the preceding procedure and contact our Support team with your Customer Id and the URL that you want to claim.

5. If you have a NetScaler Gateway installed in your on-premises setup, you can verify your URL using the following steps.

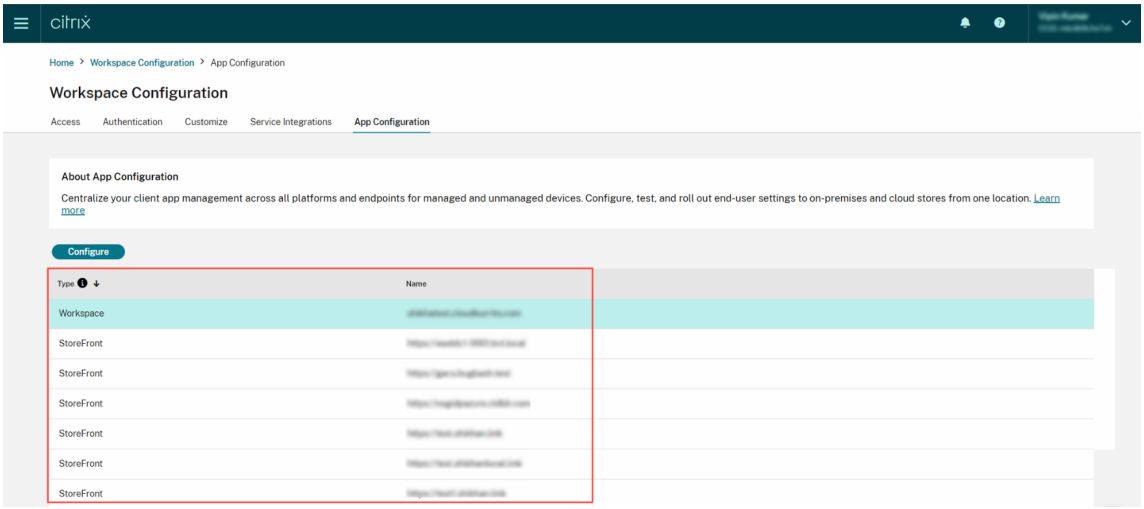
   a) **Copy** the token that appears on the pop-up.
   b) Create and configure a responder action and responder policy within your Citrix ADC.
   c) Bind your responder policy globally.
   d) Go to `https://<customergatewayurl>/vpn/CitrixClaims` to verify if your responder policy is configured correctly.
   e) Navigate back to **Claims** > **URLs**, and locate the URL that you added.
   f) Click the ellipsis menu icon for the added URL.
   g) Select **Verify URL**.
   h) Click **Start Claim Check** to start the verification process.

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

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 **Workspace Configuration** > **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.

Setup email-based discovery

Email based discovery service allows end users to sign in automatically using their email addresses. They aren't required to furnish their store URLs.
To enable this service for cloud 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

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://example.cloud.com:443`.

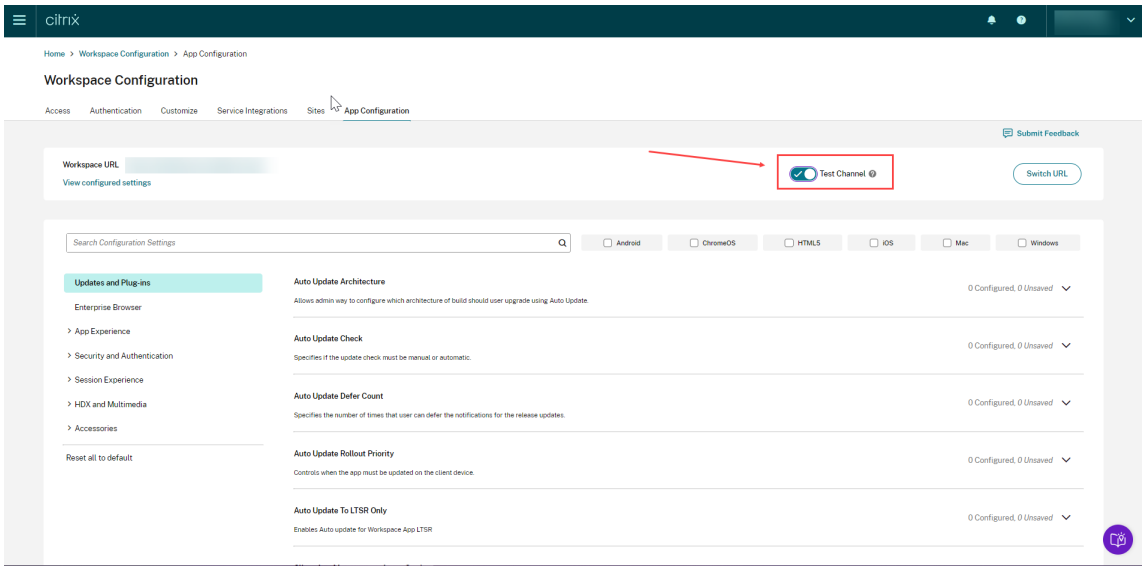
Test channel configuration

February 19, 2024

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

1. Go to the cloud portal and sign in with your Citrix Cloud credentials.
2. Navigate to **Workspace Configuration** > **App Configuration**.

3. Toggle the switch and set it to **Test Channel**. It is set to **Production** by default.



4. Modify the settings for your preferred platforms as per your requirement.
5. 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

<!--NeedCopy-->
```

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

<!--NeedCopy-->
```

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

<!--NeedCopy-->
```

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

iOS

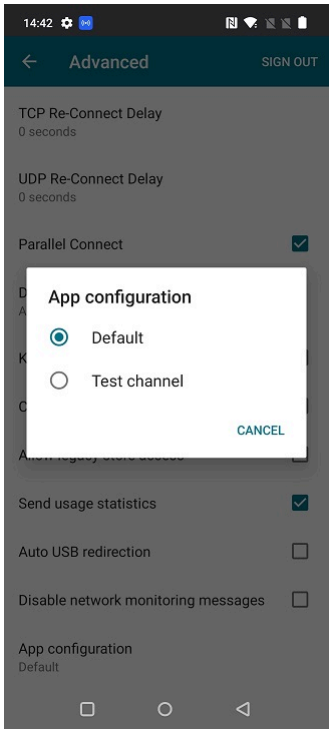
To test the configuration defined by the admin on an iOS device, proceed as follows.

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

February 19, 2024

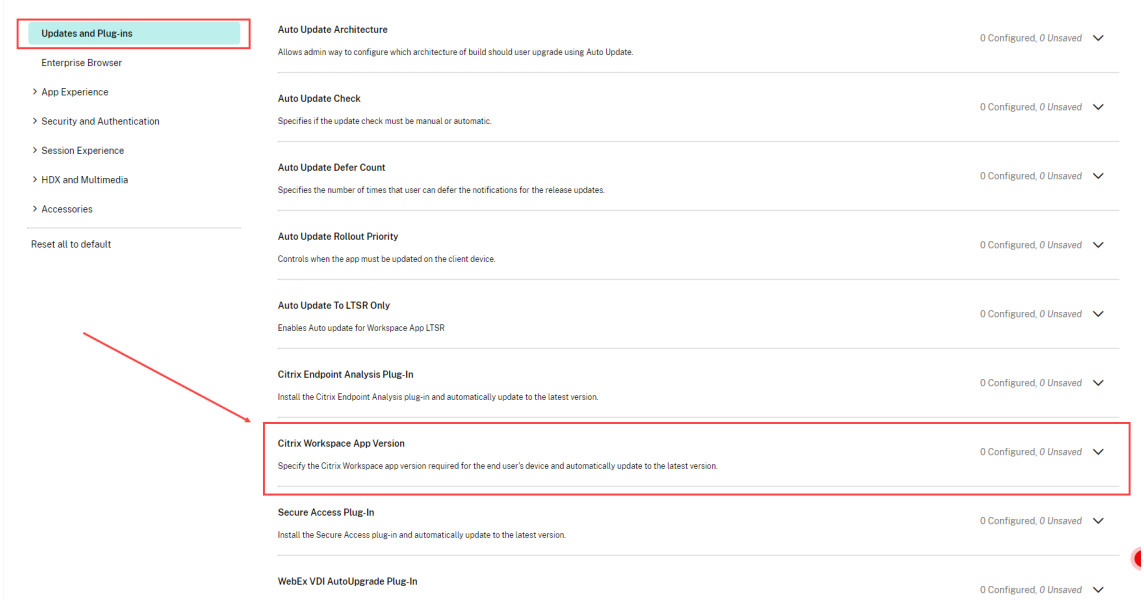
Overview

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.

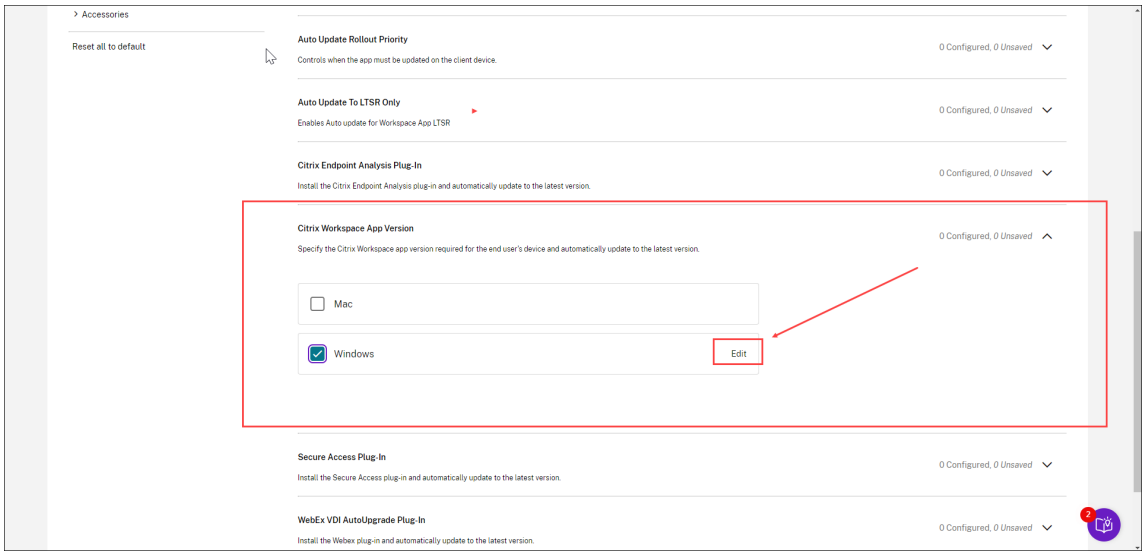
> **Note**
>
> This setting can be configured only for macOS and Windows OS.

To manage the app version settings, sign in to your Citrix Cloud console.

1. Navigate to **Workspace Configuration > 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**.



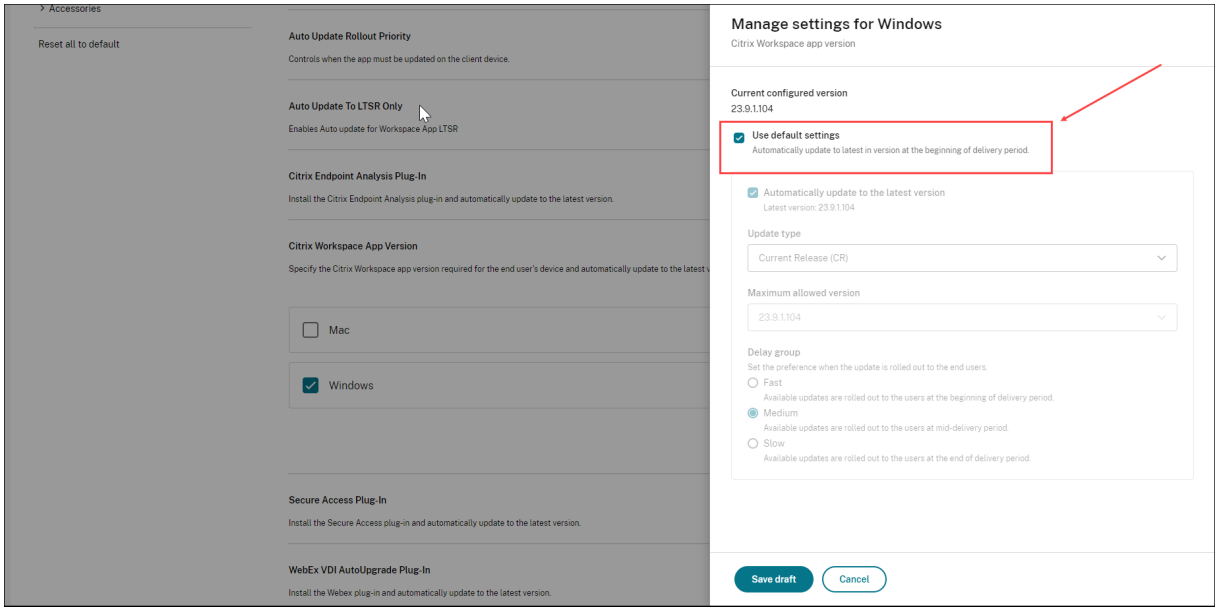
5. You can now customize the settings as explained in the Manage version settings section.
6. Save your settings.

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.

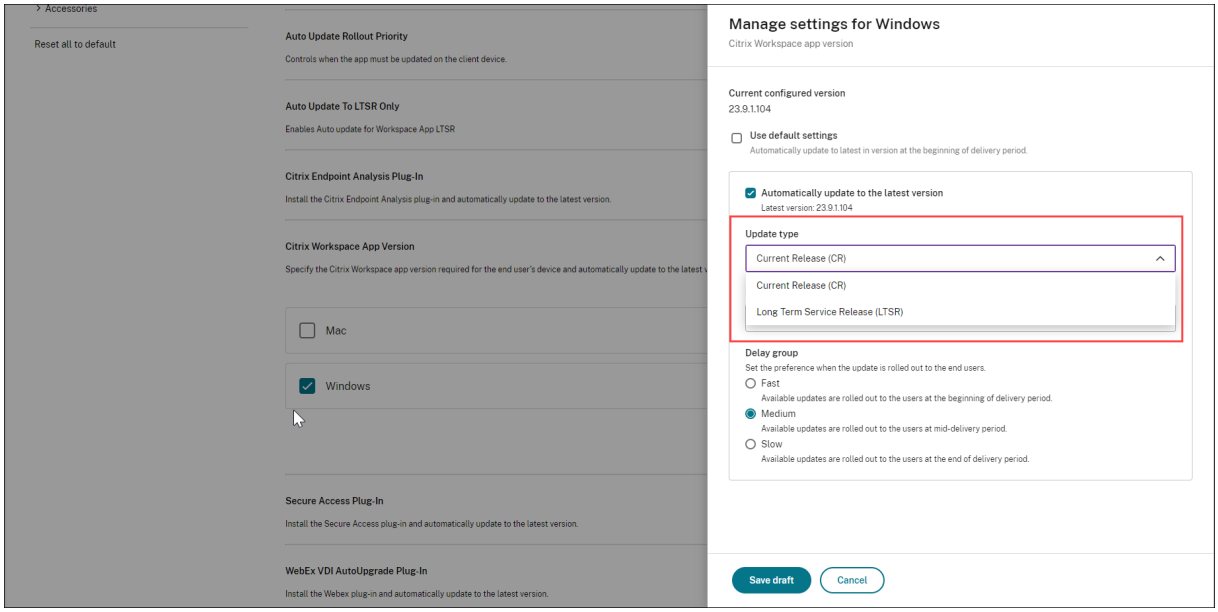


Upgrade your end users automatically to the latest LTSR or CR version

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.

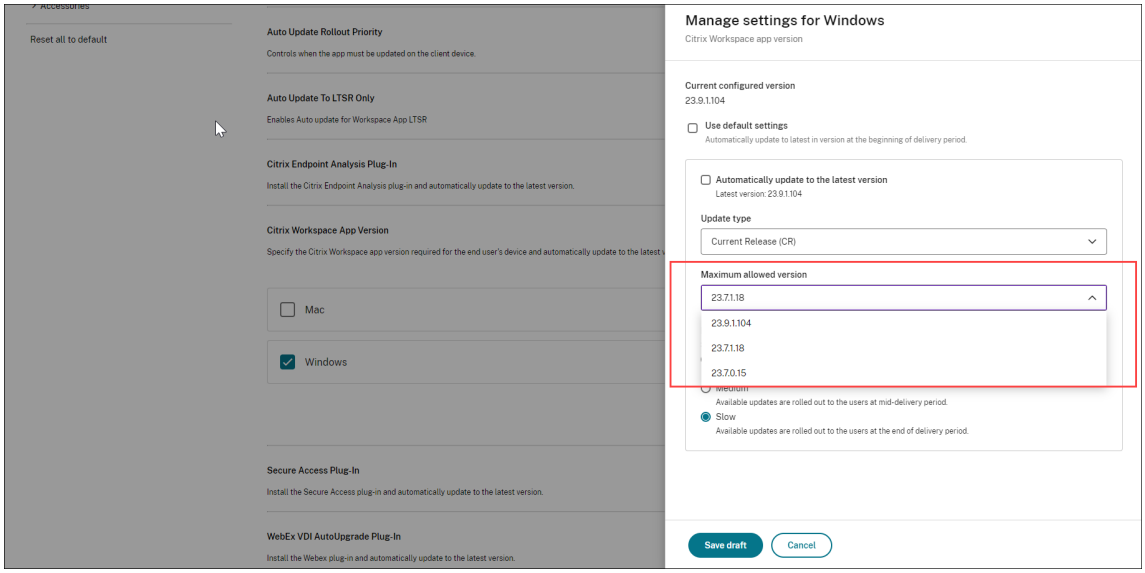


As the app is updated automatically to the latest version, the **Maximum allowed version** field is automatically disabled.

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.

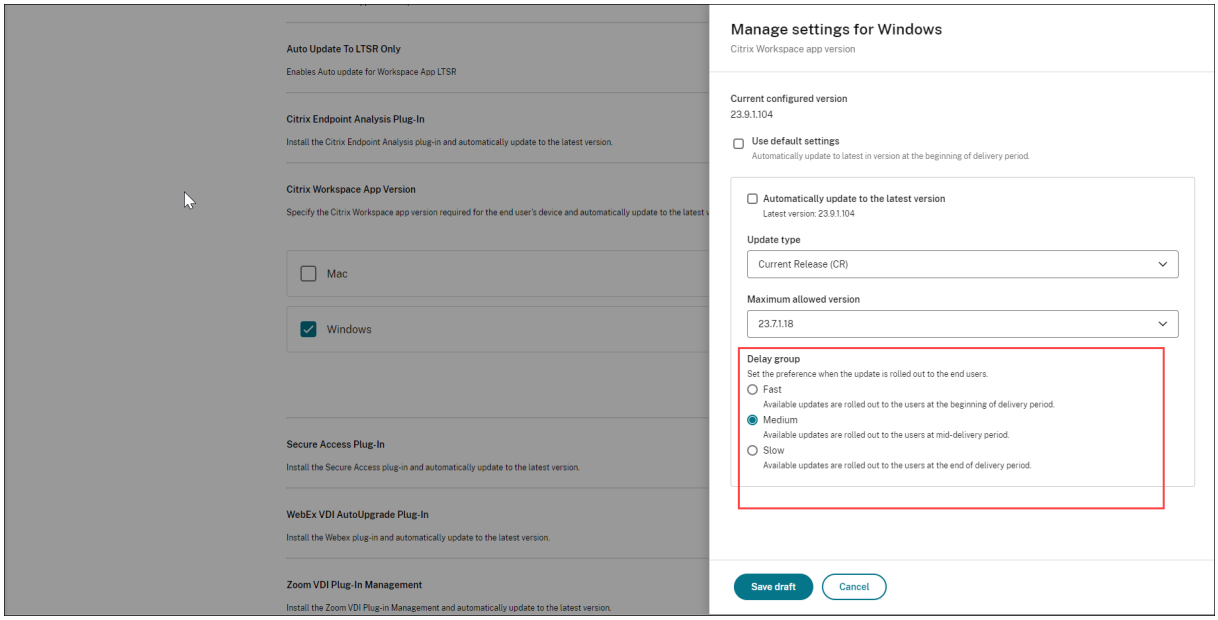


5. Under the Delay Group section, select the preferred delivery period. For more information on delivery period, see Delay Group.

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.



Manage plug-ins using Global App Configuration service

February 29, 2024

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.

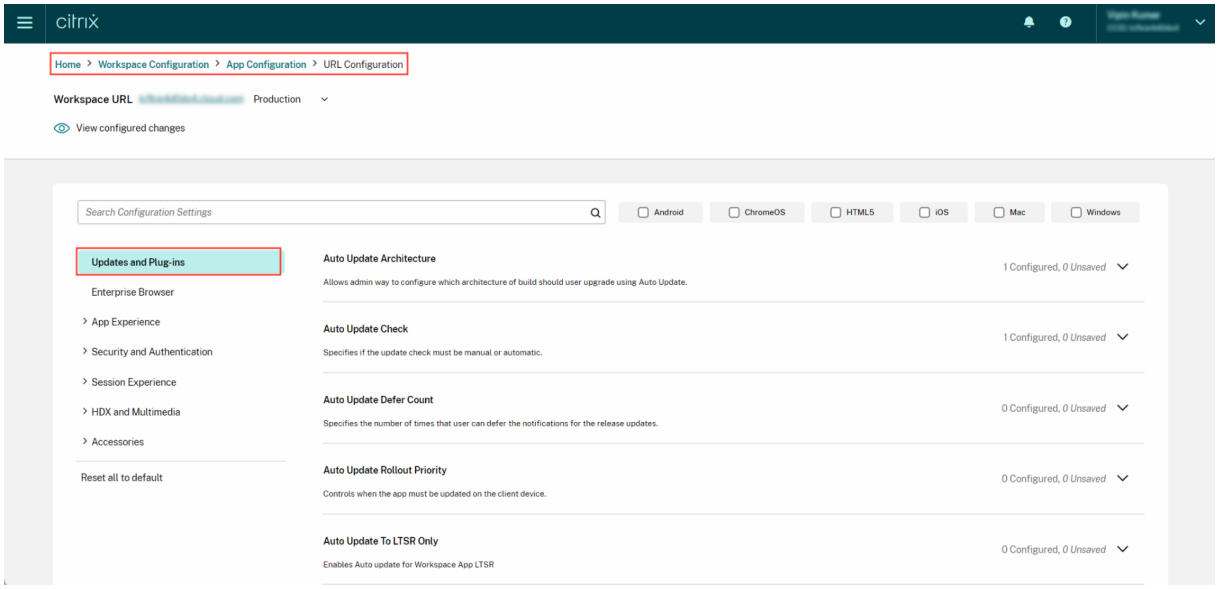
> **Note:**
>
> Plug-in installation or upgrade isn't supported for LTSR releases.

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.

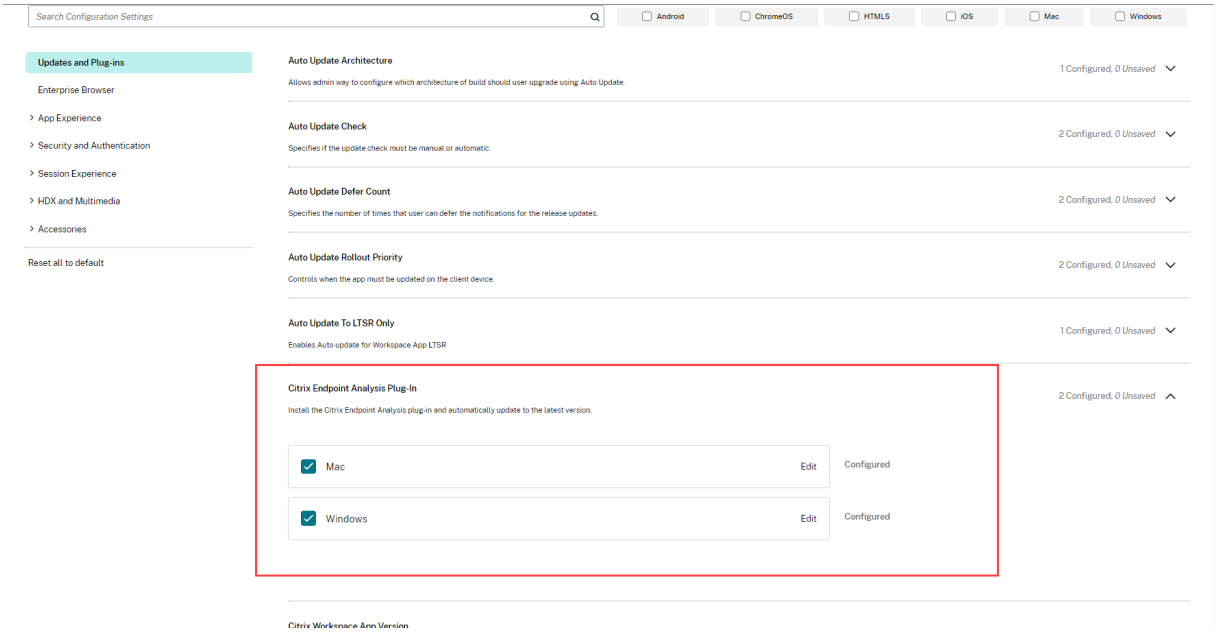
> **Note:**
>
> End users can manually update to the latest version of the plug-ins using the **Check for updates** option in their system tray. This overrides any delay group settings.
> However, this option also updates the Citrix Workspace app, either to the latest version or to the version specified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

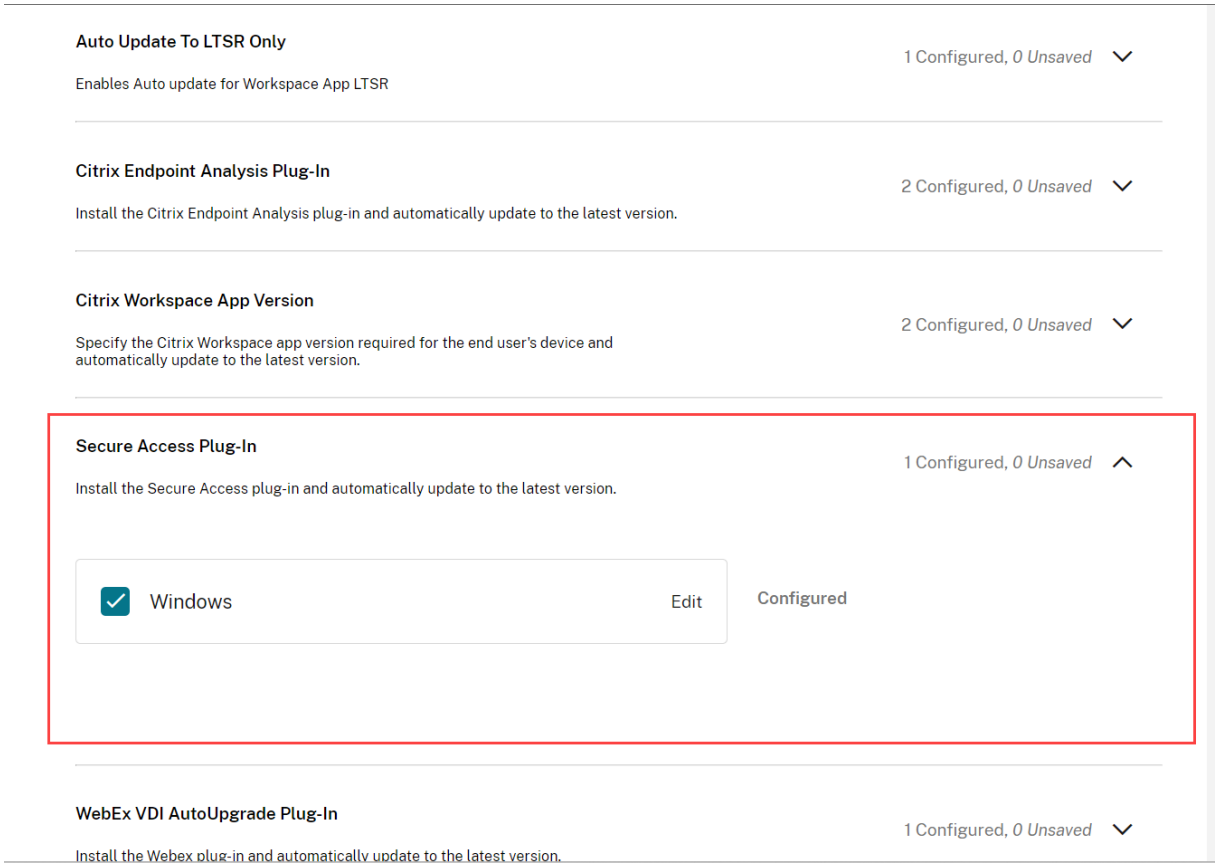
For more information, see Manage Citrix Endpoint Analysis client for Device Posture service.

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.

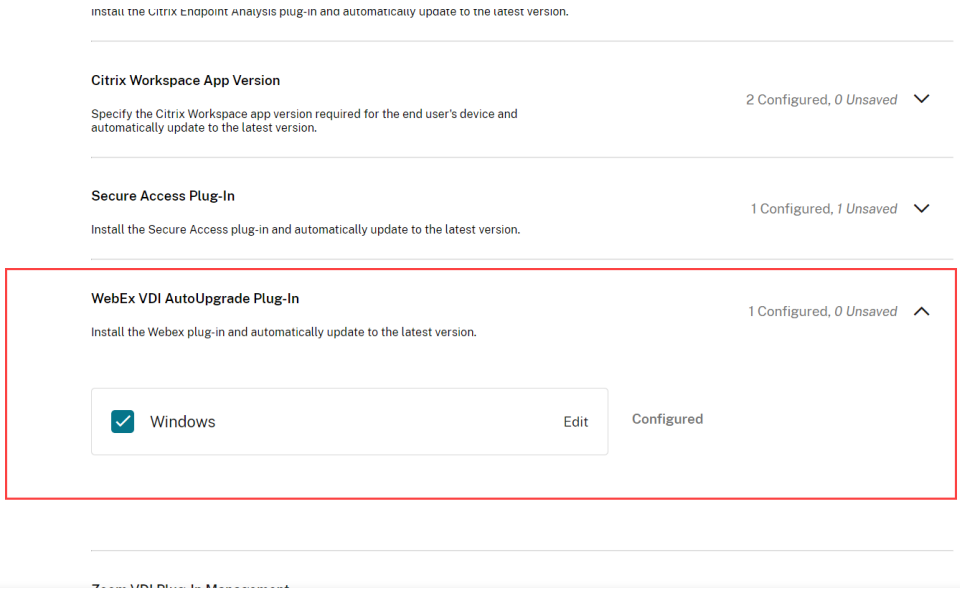
Configure plug-in settings

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:

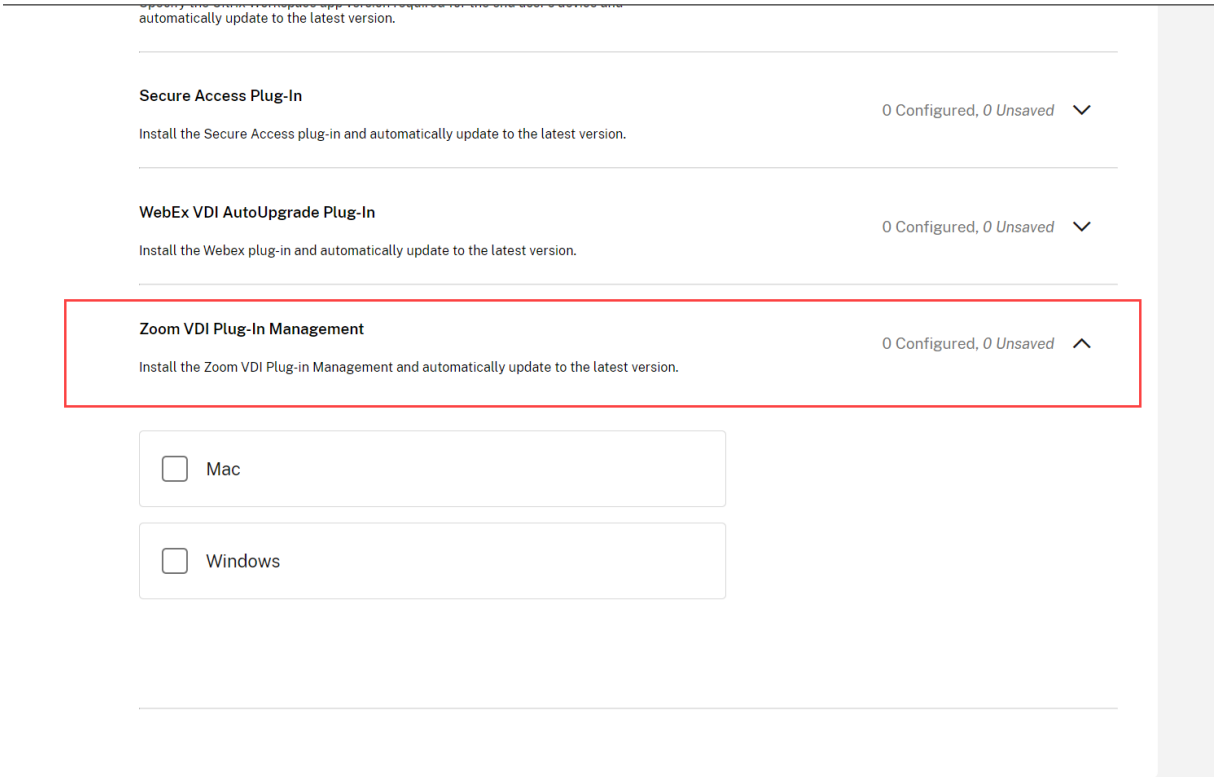
1. Go to `HKEY_LOCAL_MACHINE\Software\Cisco Spark Native\`.
2. Create a DWORD (32-bit) registry key named `VDIDisableCompatibilityVersionCheck` and give it one of these values:

```
        -   0— enables the version compatibility check (default)
        -   1— disables the version compatibility check
<!--NeedCopy-->
```

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.

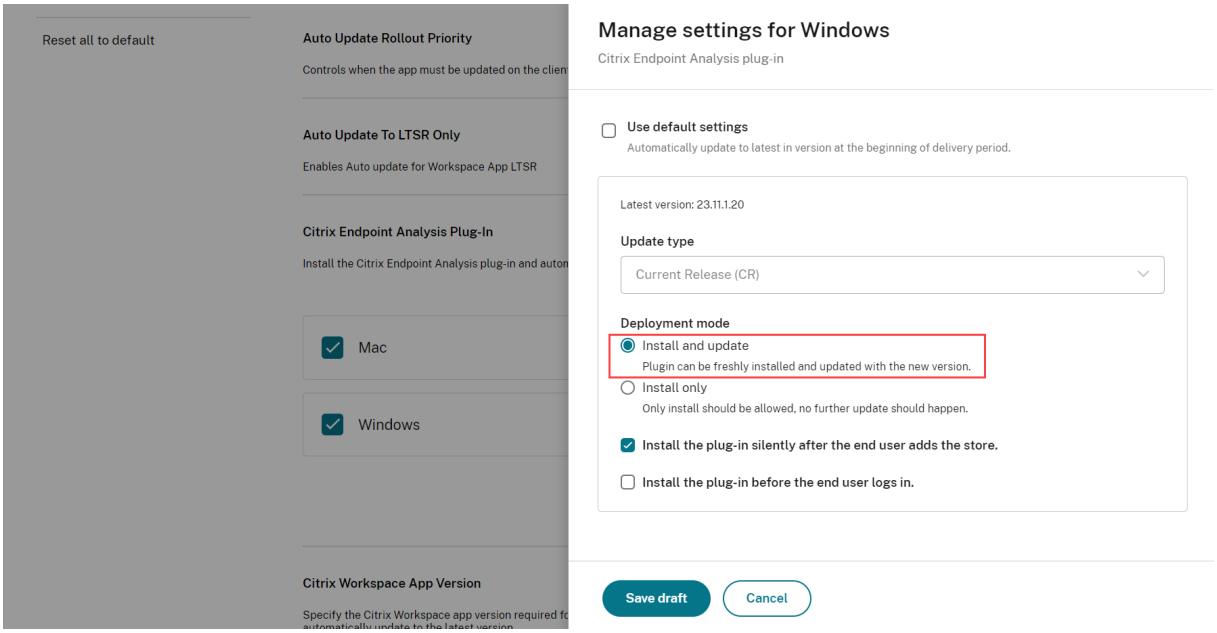
You can configure your plug-in settings as described in the Deployment mode settings section.

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.

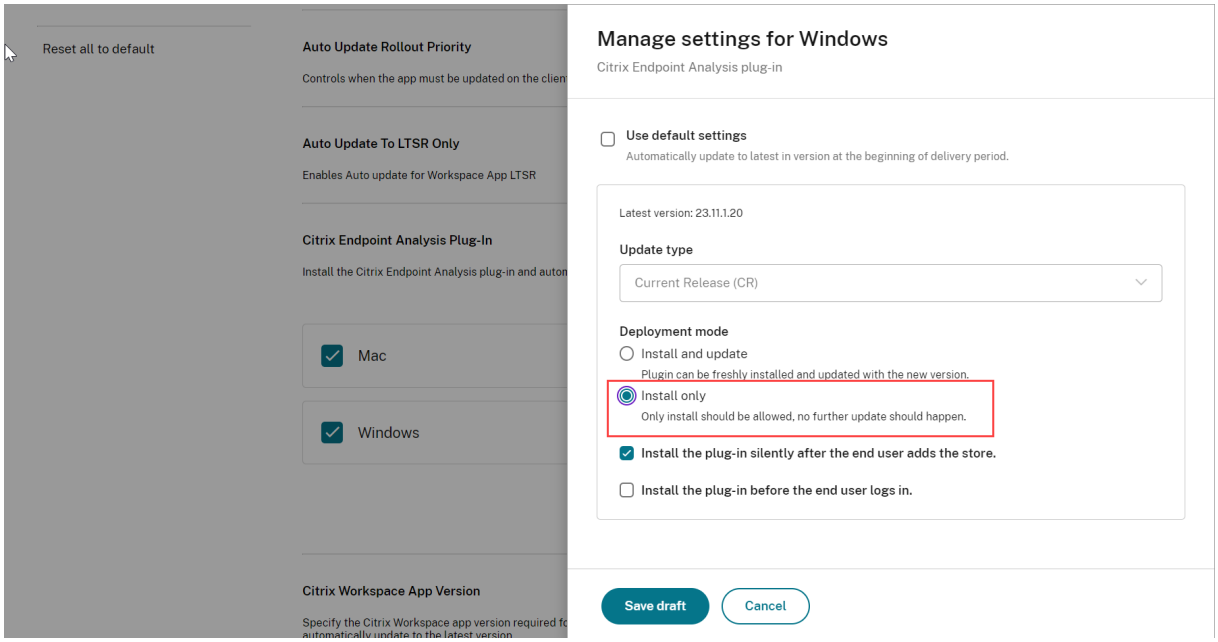
Deployment mode settings

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

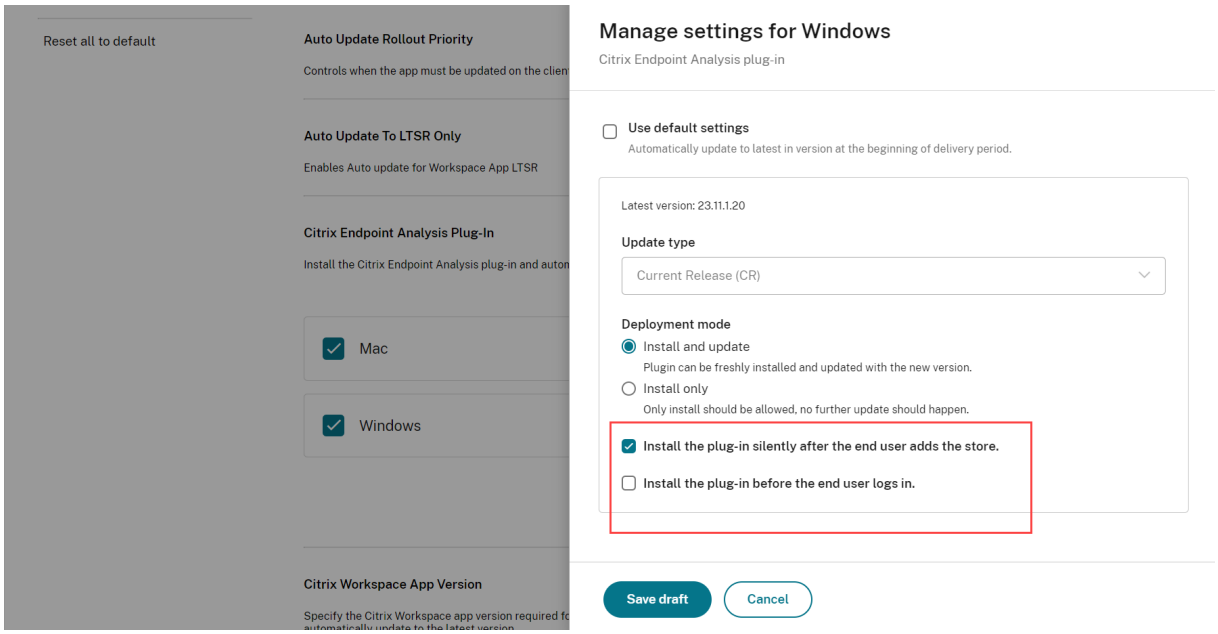
- **Install and update**: Installs the latest version of the plug-in on the end-user's device. It automatically updates the plug-in to the latest version.



- **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 your workspace experience

April 16, 2024

This article provides an overview of how subscribers can access and engage with their workspaces. It discusses customization options to enhance the workspace experience and provides solutions for common issues.

Workspace access

Subscribers can access Citrix Workspace in two ways:

- Through a browser with the Workspace URL.
- With the Citrix Workspace app, installed on subscriber devices.

Browser access

Subscribers must use the latest version of Edge, Chrome, Firefox, or Safari while signing in through the browser. Users can enter their Workspace URL to access their workspaces. For more information, see Workspace Browser Compatibility.

The workspace URL is enabled by default, usually in the format: `https://yourcompanyname.cloud.com`. For information on configuring the Workspace URL, see Workspace URL.

Citrix Workspace app access

Citrix recommends using the latest version of Citrix Workspace app to access workspaces.

The Citrix Workspace app is a natively installed app that replaces Citrix Receiver and provides a consistent user experience of the Workspace user interface (UI) across platforms. Citrix Workspace app is

available for various operating systems. For details, see the Citrix Workspace app product documentation.

If you've been using Citrix Receiver, guide users to upgrade to Citrix Workspace app so they can use all the Workspace UI features. For more information on supported features in the Citrix Workspace app by platform, see Workspace app feature matrix.

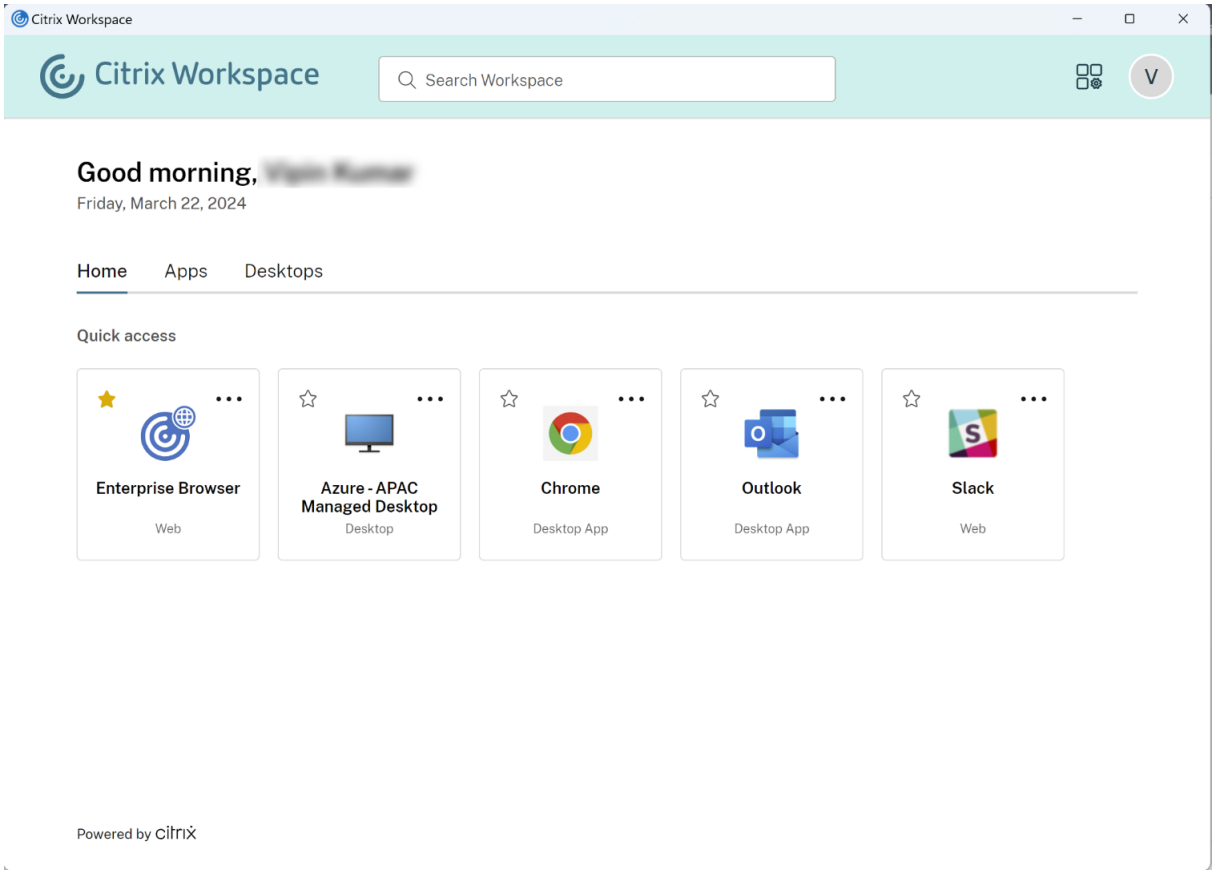
For information on how to install Citrix Workspace app, visit Download Citrix Workspace app.

For devices that can't install Citrix Workspace app software, Citrix Workspace app for HTML5 provides a connection through an HTML5-compatible browser.

Workspace user interface and features

New customers. If you're new to using Citrix Workspace app, users automatically get the latest version of the UI.

Existing customers. If you've been using an earlier version of Citrix Workspace app, the updated UI can take around five minutes to display. You might temporarily see an older version of the UI.



The Citrix Workspace UI consists of the following features:

Single sign-on (SSO)

Citrix Workspace offers a seamless experience with single sign-on (SSO) to secondary resources that otherwise require another form of authentication.

Navigation tabs

Home, **Apps**, and **Desktops** are the navigation tabs. The **Home** tab displays the most frequently used apps and desktops. When users add their favorite apps and desktops, users can quickly access them on the **Home** tab. The **Apps** tab displays a list of all available apps, and **Desktops** tab displays all available virtual desktops that users can access through Citrix Workspace app.

> **Note:**
>
> You can use the **Allow Favorites** feature in **Workspace Configuration** to configure whether users can add apps and desktops as favorites. For more information on enabling and disabling the **Favorites** feature in Citrix Workspace, see Allow Favorites.

Account Settings

Subscribers access **Account Settings** from a menu that appears when they select their profile icon in the upper-right corner of the Workspace UI.

Profile icon

You can upload a picture to the user profile. If no profile picture is set, the image defaults to an icon that is based on the user's Active Directory display name.

Search Workspace

The search tool is available at the top of the Workspace UI. The tool searches across all resources in Citrix Workspace app and allows users to open apps directly from the search results. Search requires at least three characters.

Recents and Favorites view

Subscribers can choose between a **Recents** and **Favorites** view of their apps, desktops, and files.

You can configure **Favorites** to make this feature available or unavailable to subscribers in **Workspace Configuration**. For more information on enabling and disabling the **Favorites** feature in Citrix Workspace, see Allow Favorites.

Two-factor authentication (optional)

Before subscribers can use two-factor authentication with Citrix Workspace, they must register their device. During registration, Workspace presents a QR code for the subscriber to scan with an authentication app. The authentication app must follow the Time-Based One-Time Password (TOTP) standard, such as Citrix SSO.

> **Note:**
>
> For a smooth registration process, Citrix recommends downloading and installing Citrix SSO on the target device beforehand.

To register for two-factor authentication, guide the subscriber to:

1. Open a browser, navigate to the Workspace sign-in page, and select **Don't have a token?**
2. Enter their user name in the `domain\username` format or their company email address and select **Next**. Citrix Cloud then sends the subscriber an email with a temporary verification code.
3. Enter the verification code and Active Directory account password when prompted and select **Next**.

   > **IMPORTANT:**
   >
   > The verification code is a temporary token with a 24-hour validity period and is only used to register the subscriber's device. The subscriber mustn't use this code to sign into their workspace with two-factor authentication.

4. From the authenticator app, scan the QR code or enter the verification code manually.
5. Select **Finish** and **Sign In** to complete the registration.

After completing registration, subscribers can return to the Citrix Workspace sign-in page and enter their Active Directory credentials along with the token displayed in their authentication app.

Only verification codes that are generated from an authentication app on an enrolled device are supported tokens for two-factor authentication. Subscribers mustn't use the temporary email token sent during the registration process.

Customize workspaces

You can customize the subscriber experience of workspaces for different users and to meet specific organizational requirements in **Workspace Configuration**.

- To customize the appearance of workspaces, including logos and custom themes, visit Customize the appearance of workspaces.

- To choose how subscribers interact with their workspaces, such as allowing subscribers to create **Favorites** and automatically launching desktops, visit Customize workspace interactions.
- To customize privacy and security policies, see Customize security and privacy policies. The privacy and security policies include settings such as timeout period, sign-in policy, and password management for end users.

Troubleshooting

Log out and back in after changing authentication method

After you've changed the authentication method, subscribers that are logged in might see an error message. Subscribers must log out of Citrix Workspace and close the browser or Citrix Workspace app, and wait approximately 5 minutes to log in again. Subscribers can then sign in using the new authentication method.

For more information, visit Choose or change authentication methods.

Refresh after changes to your service subscription

If you've changed your service subscription, subscribers might need to manually refresh the local Citrix Workspace app. To refresh the Citrix Workspace app for Windows:

1. Right-click the Citrix Workspace icon in the Windows system tray and select **Advanced Preferences > Reset Citrix Workspace**.
2. Open Citrix Workspace app for Windows and select **Accounts > Add**.
3. Enter the Workspace URL and then select **Add**.

You can also refresh the Citrix Workspace app from the browser. If refreshing from the browser:

1. Right-click the Citrix Workspace icon in the Windows system tray and select **Advanced Preferences > Reset Citrix Workspace**.
2. Enter the Workspace URL into the browser and sign in.
3. Download the configuration file from **Settings > Account Settings > Advanced > Download Workspace Configuration**.

This downloads a file with a **.cr** extension that adds the workspace to your local Citrix Workspace app.

Customize the appearance of workspaces

February 19, 2024

Customize the Workspace user interface

This section describes how you can customize the appearance of workspaces by updating themes in **Configuration > Customize > Appearance**.

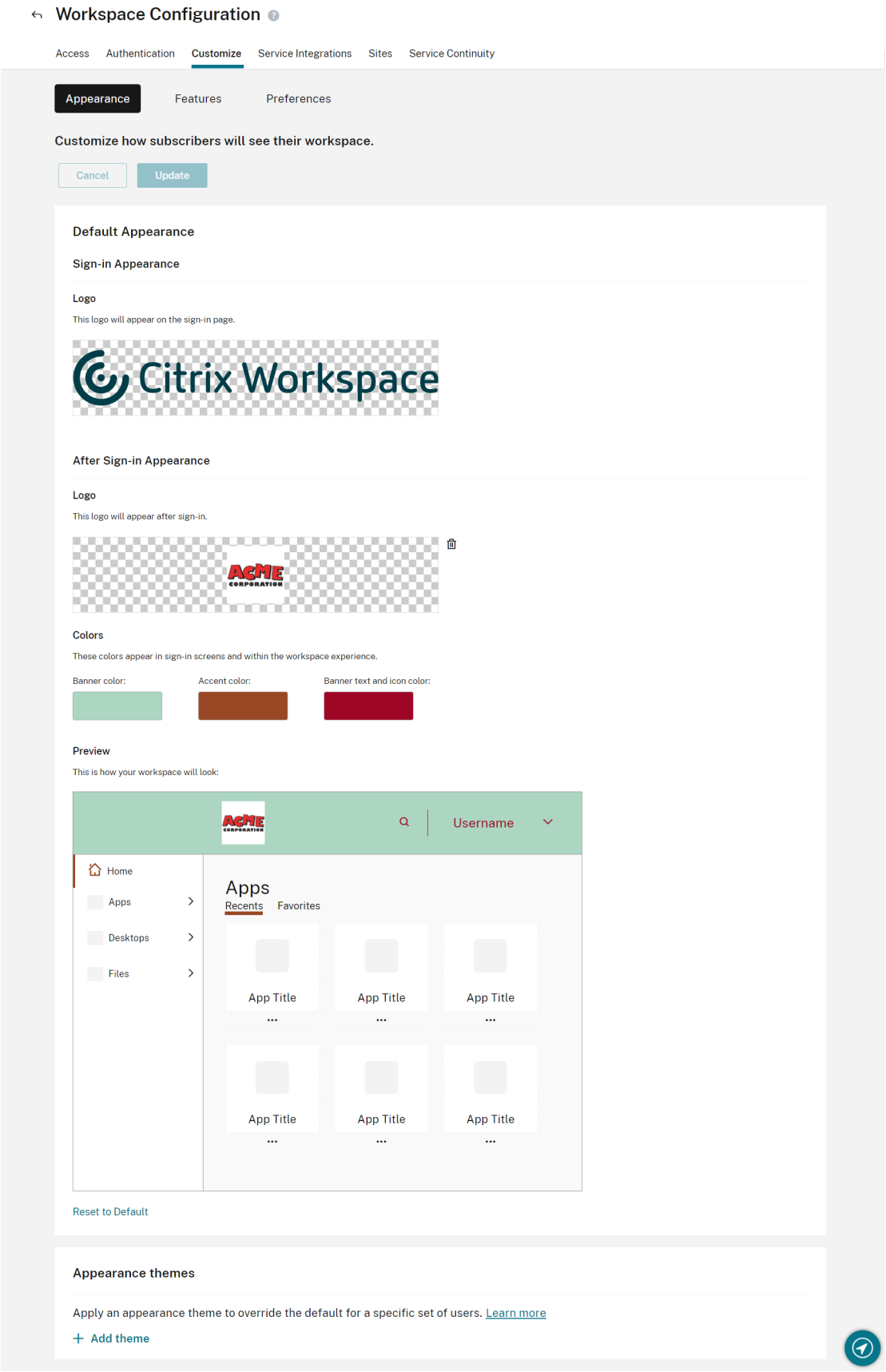
Themes allow you to configure your workspace colors and logos. Logos must meet the required dimensions to avoid appearing distorted or resulting in an error message.

Logo	Required dimensions	Max. size	Supported formats
Sign-in logo	480 x 120 pixels	2 MB	JPEG, JPG, or PNG
Post sign-in logo	340 x 80 pixels	2 MB	JPEG, JPG, or PNG

Changes to the workspace appearance take effect immediately after you select **Save**.

Customize your default theme

The default theme includes the sign-in logo, and the workspace logo and colors that subscribers see after they sign in. You can change one, some, or all of these elements for the default theme.



Customize 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.

Changes to the workspace appearance take effect right away. It can take around five minutes for the updated user interface to appear in local Citrix Receiver apps.

> **Note:**
>
> Changes to the sign-in logo don't impact users who authenticate to their workspace using third-party identity providers, such as Azure AD and Okta.
>
> For information on how to customize an Azure AD 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 **Workspace Configuration**. For more information, see the Support Knowledge Center article.

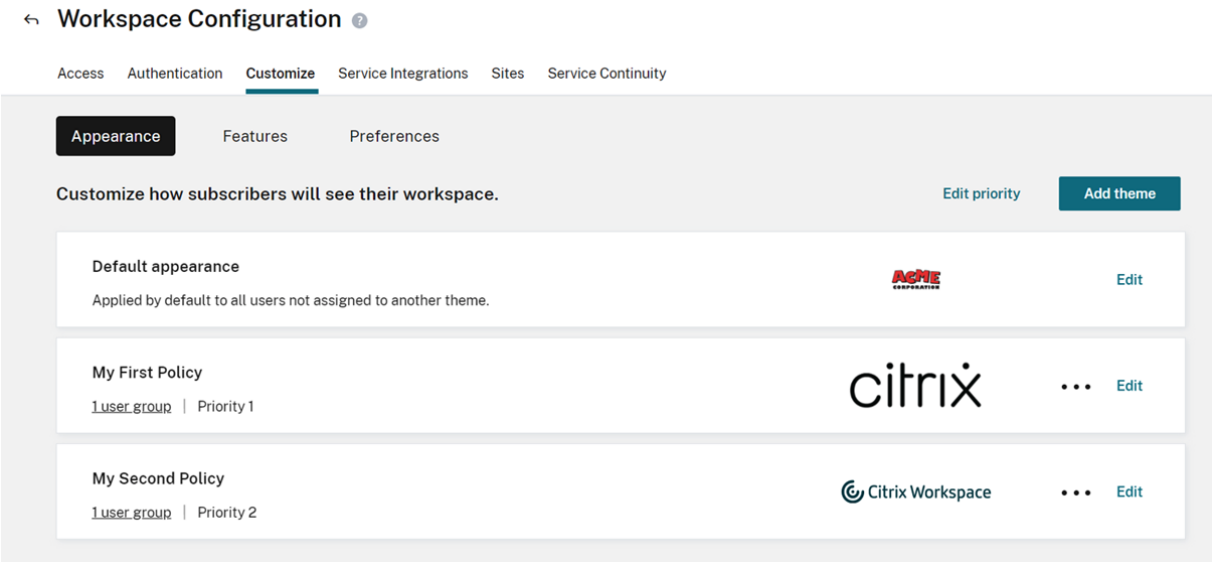
Customize the workspace appearance

The sign-in logo doesn't have to be the same as the logo that appears at the top left of the workspace after a subscriber signs in. In addition to replacing the workspace logo, you can define the banner, accent, and text and icon colors of the workspace.

Create multiple custom themes

> **Important:**
>
> The Multiple custom themes feature is available as a **single-tenant** feature. If your customer is a Citrix Service Provider tenant, it must have its own resource location, Cloud Connectors, and dedicated Active Directory domain. Citrix Service Provider tenants that share a resource location, Cloud Connectors, and dedicated Active Directory domain (multitenancy) aren't currently supported.

You can configure and prioritize multiple Citrix Workspace themes for specific user groups. These custom themes are listed in individual cards under the default theme. If you don't set up multiple themes, the existing (default) theme is applied to all users.



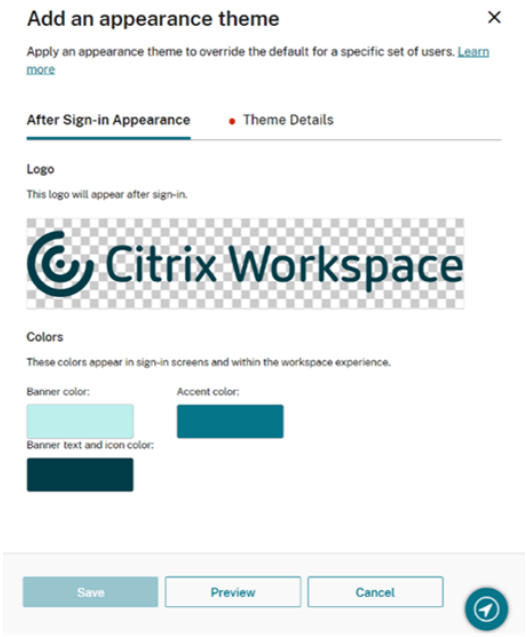
Configure custom themes

To add your first custom theme under your default theme, select **Add theme** at the bottom left of the card under the **Default appearance** section.

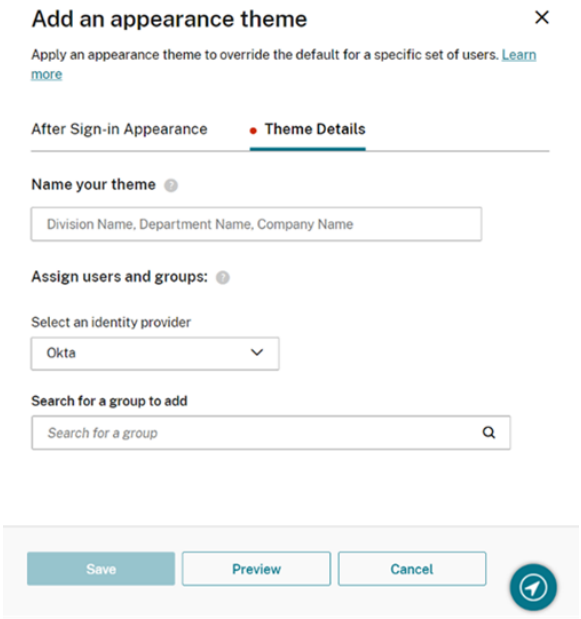
If you already have at least one custom theme under the default theme, select **Add theme** at the top right of the list of existing themes.

1. Configure your custom theme:

    a) Upload your **Logo** (optional).
    b) Define your banner, accent, and text and icon **Colors** (optional).



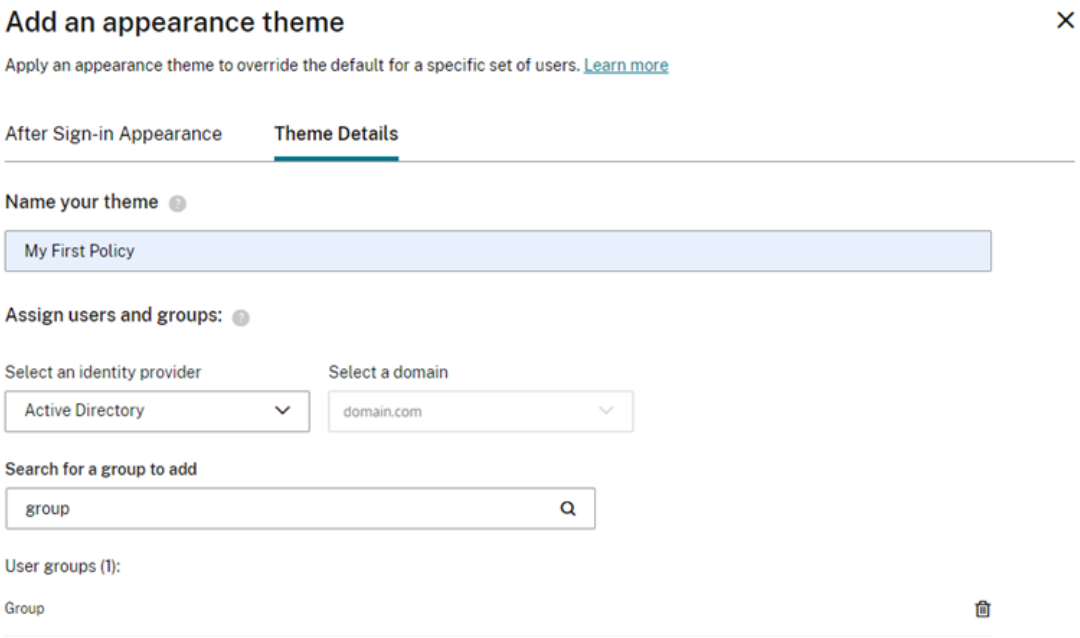
2. Select **Theme Details** and enter a meaningful name for the theme.



3. 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 add to your theme.



4. Select **Preview** to see how your workspace looks to subscribers. Save your theme changes when you're done.

   > **Note:**
   >
   > **Workspace Preview** doesn't show a preview if you're currently working with the older purple user interface.

5. Repeat steps 1 through 4 to continue adding new custom themes.

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 which theme a subscriber sees if they match to more than one user group. It can be achieved by setting the priority of custom themes relative to one another.

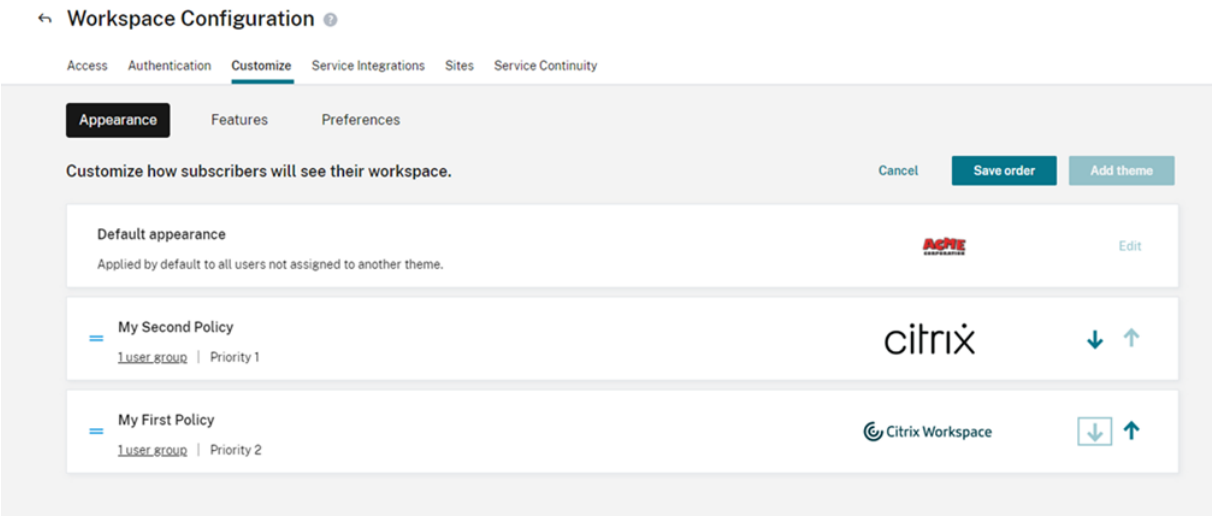
> **Important**
>
> For relative prioritization of custom themes to work, you must configure two or more custom themes under the default theme.

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**.



Customize workspace interactions

April 16, 2024

Customize how subscribers interact with their workspaces in **Workspace Configuration > Customize > Preferences**.

If you want to customize workspace preferences that affect the sign-in experience to align with your company requirements, visit Customize workspace security and privacy policies.

If you want to customize the pre-login and post-login workspace appearance, visit Customize the appearance of workspaces

Allow Caching

The **Allow Caching** setting enhances performance for subscribers accessing Citrix Workspace through a web browser. Caching is supported when accessing Citrix Workspace with a supported web browser. Caching isn't available when using a locally installed Citrix Workspace app.

When caching is enabled, some sensitive data might be stored locally on subscribers'devices. This data consists of file metadata and is encrypted with a key that's unique to the subscriber's authenticated identity. The encrypted data is stored in the web browser's `localStorage` property on the subscriber's device.

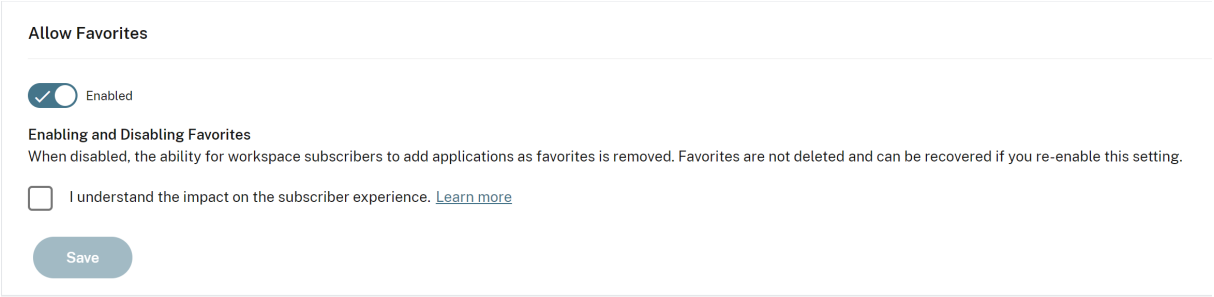
If you disable caching, the encrypted data is purged the next time the subscriber signs in to Citrix Workspace through their web browser. Also, the subscriber can purge this data manually by clearing browsing data from their web browser.

Allow Favorites

Customers, who have access to **Workspace Configuration** and the new Workspace 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:

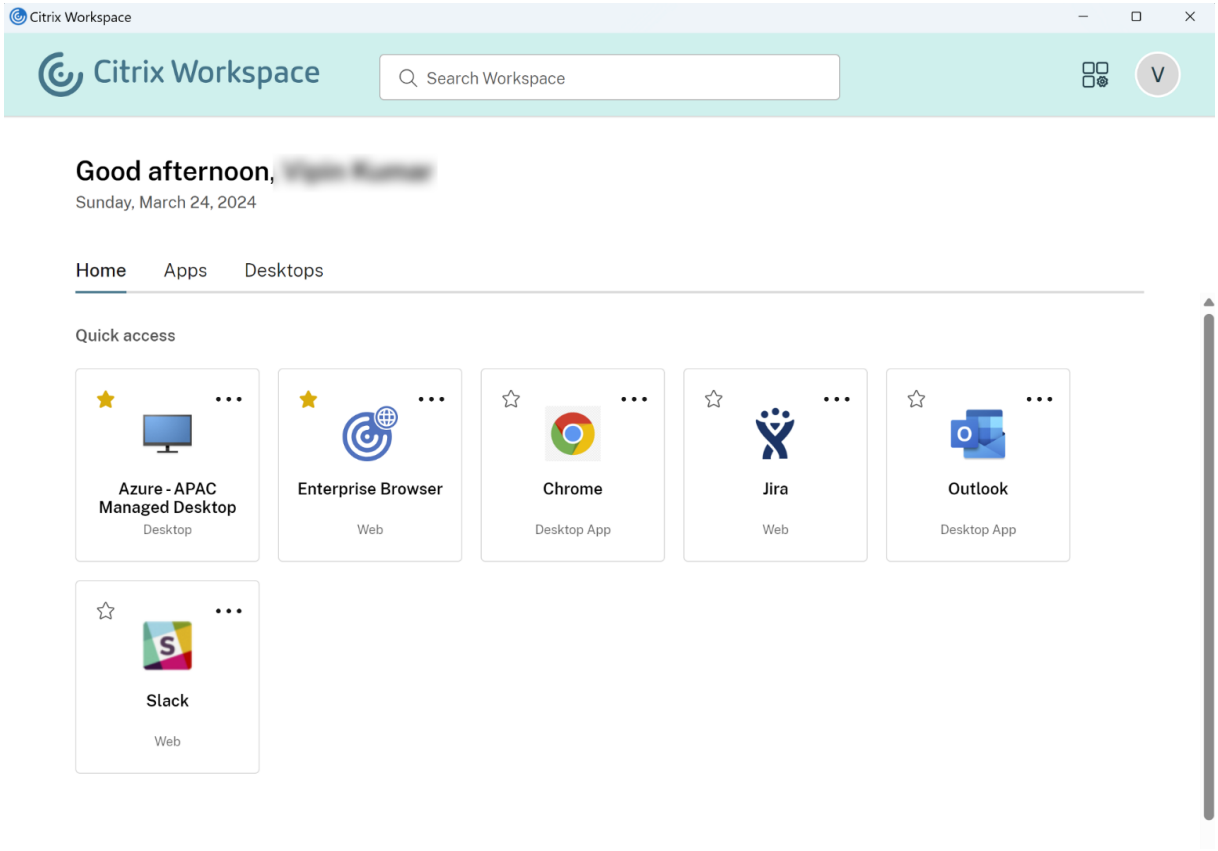
1. Navigate to **Workspace Configuration** > **Customize** > **Preferences**.
2. Click the toggle button to enable or disable the feature.
3. Select the declaration checkbox, and click **Save**.



> **Note:**
>
> For some existing customers (new to Workspace between December 2017 and April 2018), **Allow Favorites** defaults to **Disabled**. You can decide when to enable this feature for your users.

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.



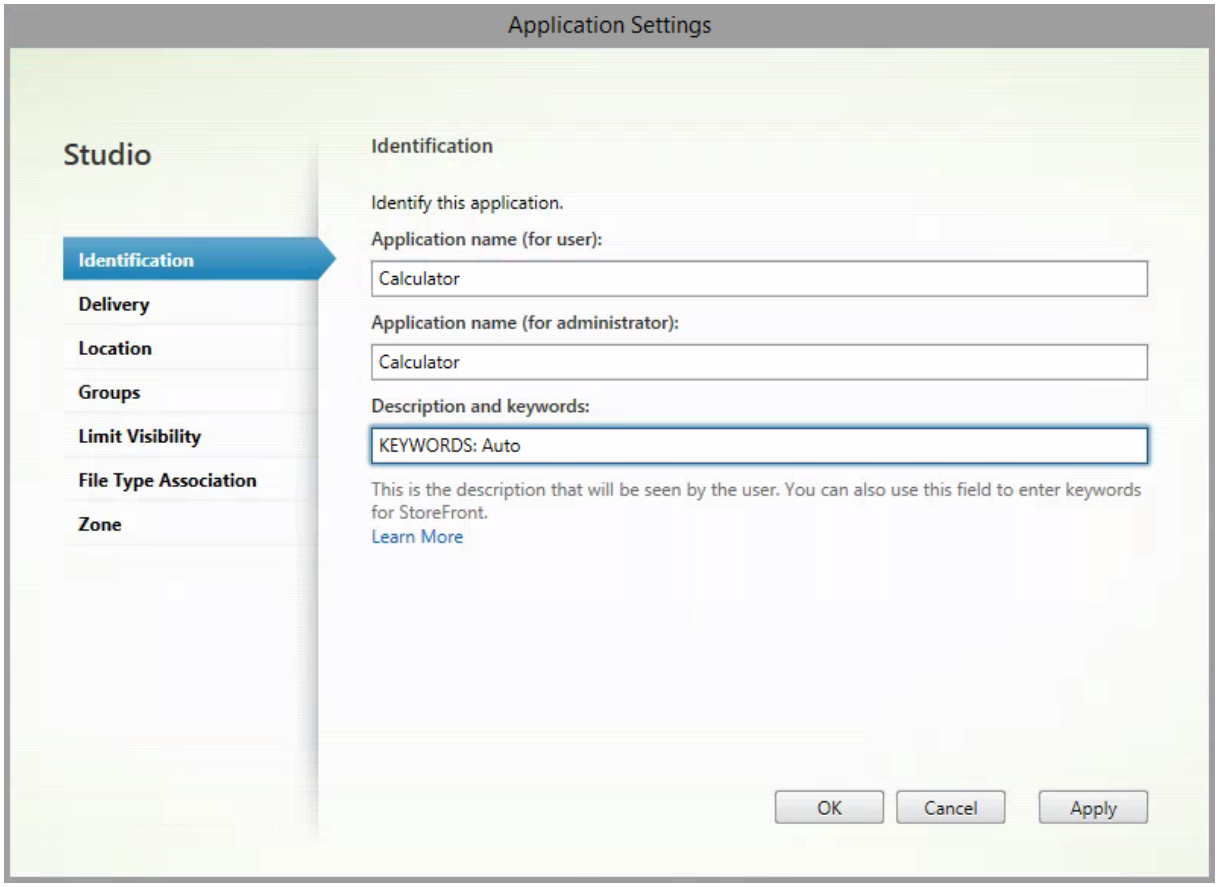
When a user adds more than 250 favorite resources, the oldest favorite resource is removed (or as close as possible) to preserve the most recent favorite resources.

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.

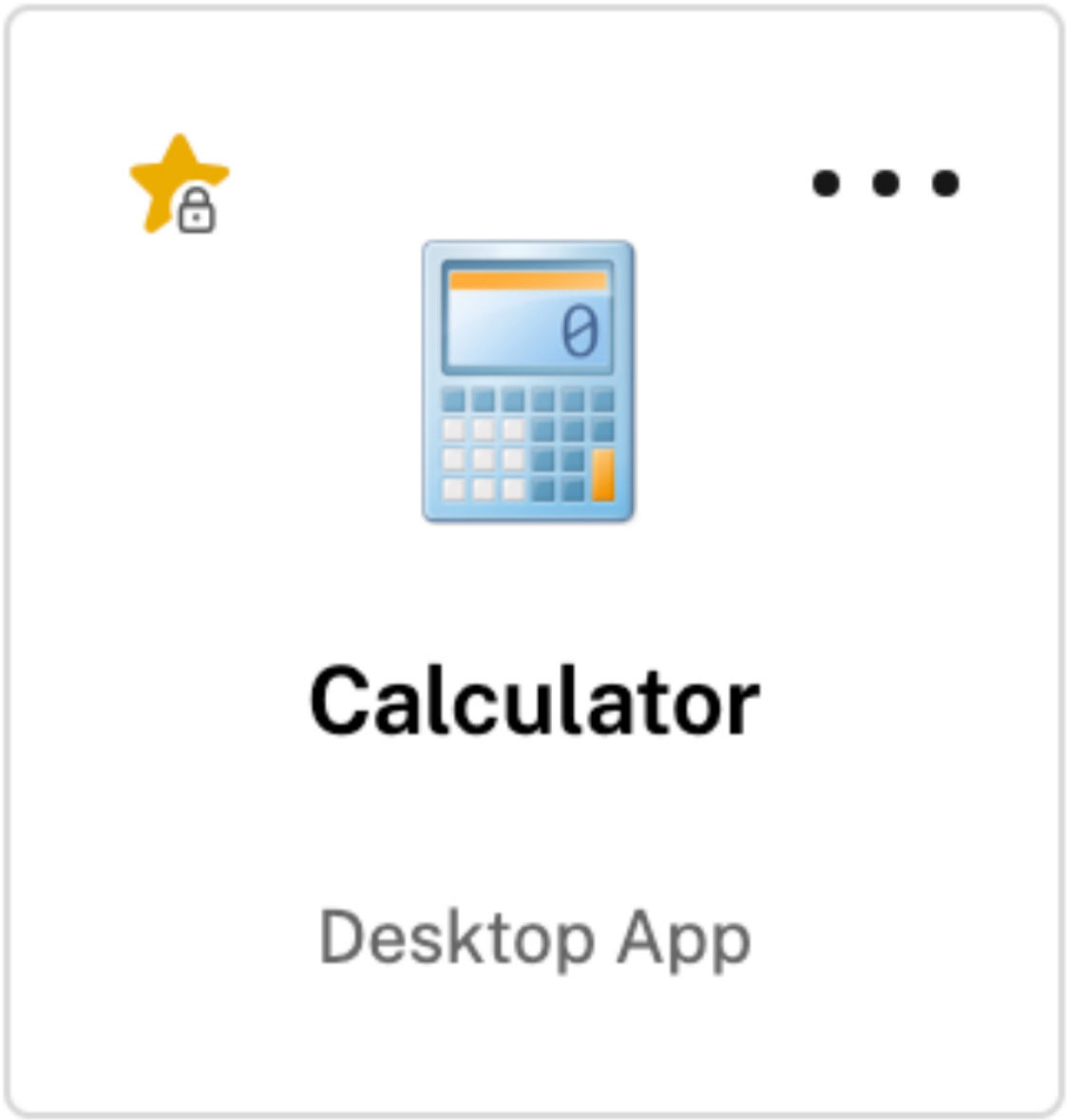
> **Note:**
>
> - **Allow Favorites** feature is enabled by default.
> - If your users don't have access to the desktops configured, the **Desktop** tab doesn't appear on the navigation bar.

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.

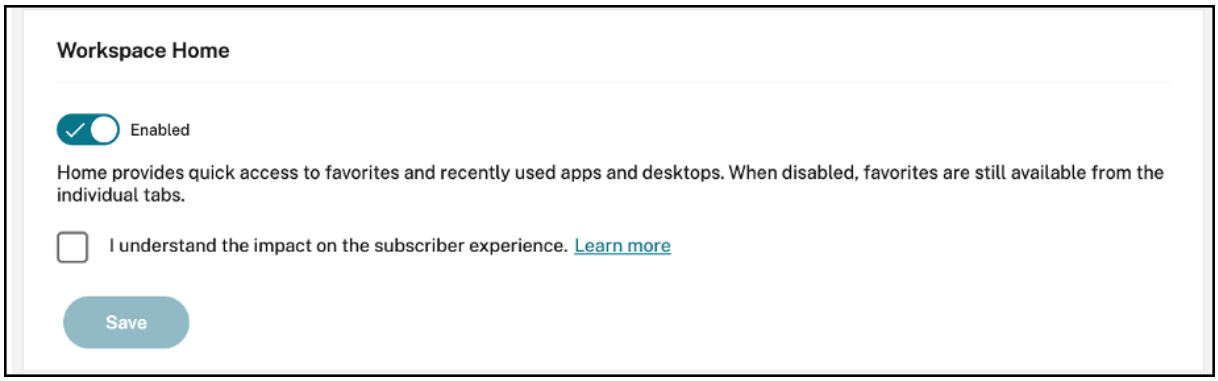
Enable or disable Home screen for users (Preview)

You can enable or disable the **Home** page for your users to improve the organization of their apps.

This feature is applicable when users have more than 20 apps on their desktop. If the users have 20 apps or less, then they see a single view with no navigation and search options.

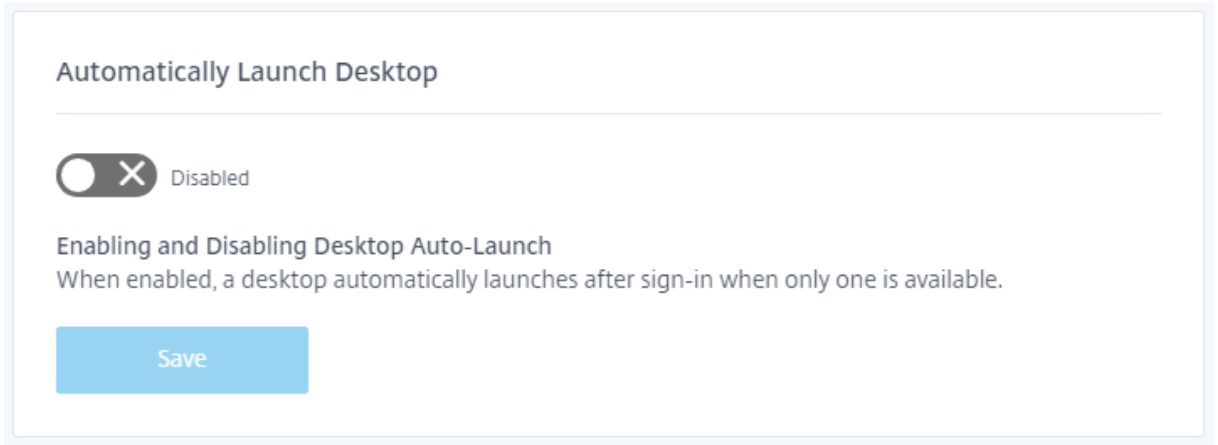
To configure the settings, navigate to **Workspace configuration > Customize > Appearance**. When

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.



Automatically Launch Desktop

Automatically Launch Desktop is available to customers who have access to **Workspace Configuration** and the new Workspace experience. The preference only applies to workspace access from a browser.



When disabled (default), the setting prevents Citrix Workspace from automatically starting a desktop when a subscriber signs in. Subscribers must manually launch their desktop after signing in.

When enabled, if a subscriber has only one available desktop, the desktop automatically launches when the subscriber signs in to their workspace.

The subscriber's applications aren't reconnected, regardless of the Workspace control configuration.

> **Note:**
>
> To enable Citrix Workspace to launch desktops automatically, subscribers accessing the site through Internet Explorer must add the Workspace URL to the Local intranet or Trusted sites

> zones.

Federated identity provider sessions

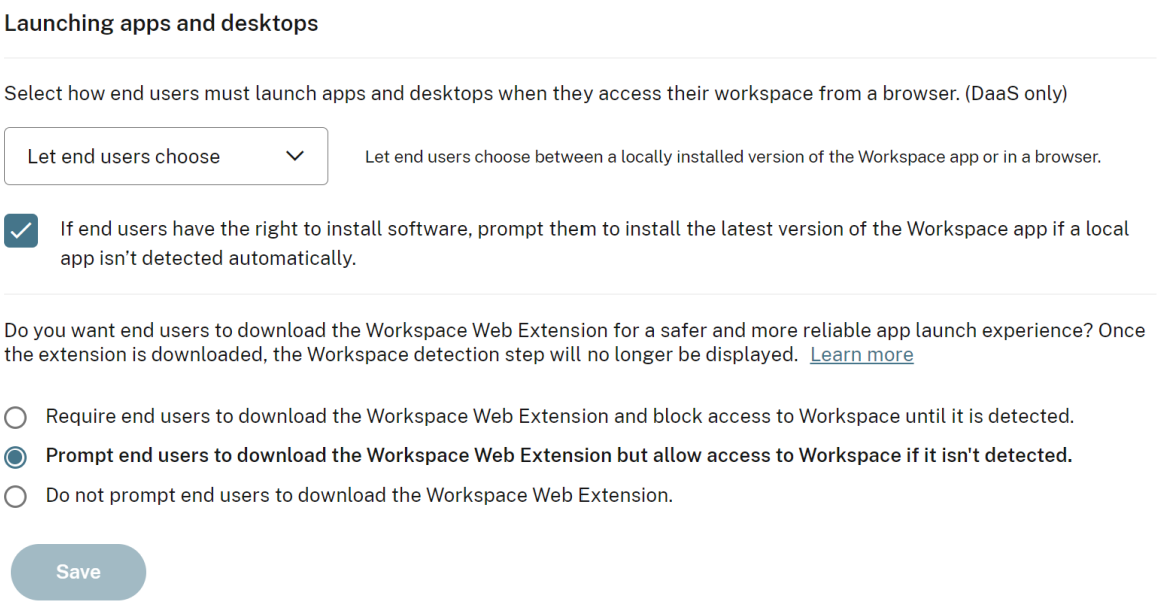
When Workspace is configured to use a federated identity provider, the authentication session and its lifetime are typically controlled by the identity provider. The **Federated Identity Provider Sessions** setting allows the control to be handed off to the Service Provider. When enabled (default), Workspace forces a sign-in prompt with the identity provider when a new Workspace session is needed. When disabled, a subscriber won't be prompted to authenticate with the identity provider if accessing Workspace with a valid session.

If this setting is enabled and you're using Azure AD for workspace authentication, subscribers might be prompted to sign in again even if a valid Microsoft authentication token exists for their session. For more information about this scenario, see CTX253779.

Launching apps and desktops

The **Launching apps and desktops** setting is available to customers who have access to **Workspace Configuration** and the new Workspace experience. The preference is available to new and existing customers. However, the introduction of this feature doesn't change any settings for existing customers.

The preference applies to the way users open apps and desktops delivered by **Citrix DaaS** only. This can be the **Citrix DaaS** service or on-premises from the Site aggregation feature. **Launching apps and desktops** doesn't apply, for example, to SaaS apps delivered by the Citrix Gateway service.



Choose one of the following settings:

- **In a native app** (default): End users are required to use a locally installed version of the Workspace app.
- **In a browser:** End users are required to use a browser version of the Workspace app for HTML5.
- **Let end users choose:** End users can choose between a locally installed version of the Workspace app or launch apps and desktops in a browser.

An additional option for **In a native app** and **Let end users choose** prompts users to install the latest version of Citrix Workspace app if a local app isn't detected automatically. Remove this selection if your subscribers don't have the rights to install software.

Manage installation prompt for Workspace Web Extension

Workspace can detect whether a user has installed Workspace Web Extension on their device or not. If not, Workspace prompts the user to download and install the extension. The Workspace detection step doesn't get displayed if the user installs the extension.

To manage installation prompt for Workspace Web Extension, navigate to **Workspace Configuration** > **Customize** > **Preferences** > **Launching apps and desktops**, and then choose one of the following settings:

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

Integrate Microsoft Teams with Workspace

With the Microsoft Teams integration, subscribers can share cards from their Workspace **Activity Feed** with other subscribers through channels in Microsoft Teams.

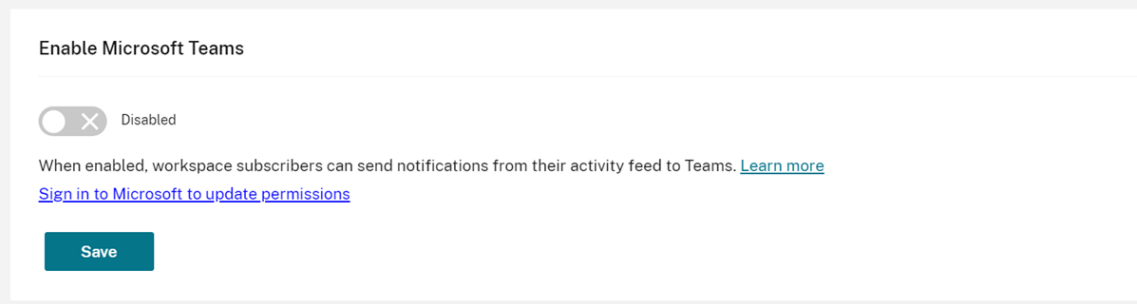
Requirements

- You must be a **Full Access** administrator in Citrix Cloud to enable Microsoft Teams integration. Administrators with **Custom Access** don't have the required permissions to enable Microsoft Teams integration.

- You must configure Azure AD authentication in **Identity and Access Management**. For more information about configuring Azure AD authentication, see Connect Azure Active Directory to Citrix Cloud.
- You can use only one Azure AD instance with Microsoft Teams. If the Azure AD instance you configure has Microsoft Teams enabled through another Citrix Cloud account, you can't enable Microsoft Teams integration for your Citrix Cloud account.
- The feature toggle **IwsMicrosoftTeams** must be enabled.
- You must have the **Actions and Activity Feed** feature enabled for workspaces.
- Workspace subscribers must have the Microsoft Teams desktop client installed.

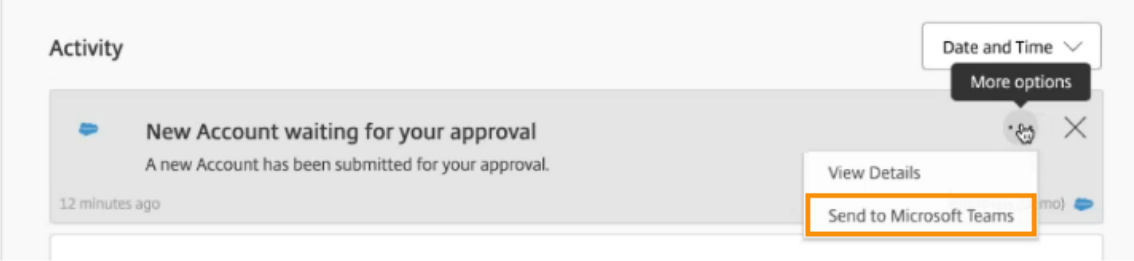
Enable Microsoft Teams integration

1. After signing in to Citrix Cloud, select **Workspace Configuration**.
2. Select **Customize**, and then the **Preferences** tab.
3. Under **Enable Microsoft Teams**, select the toggle to enable.



4. Select **Save**.

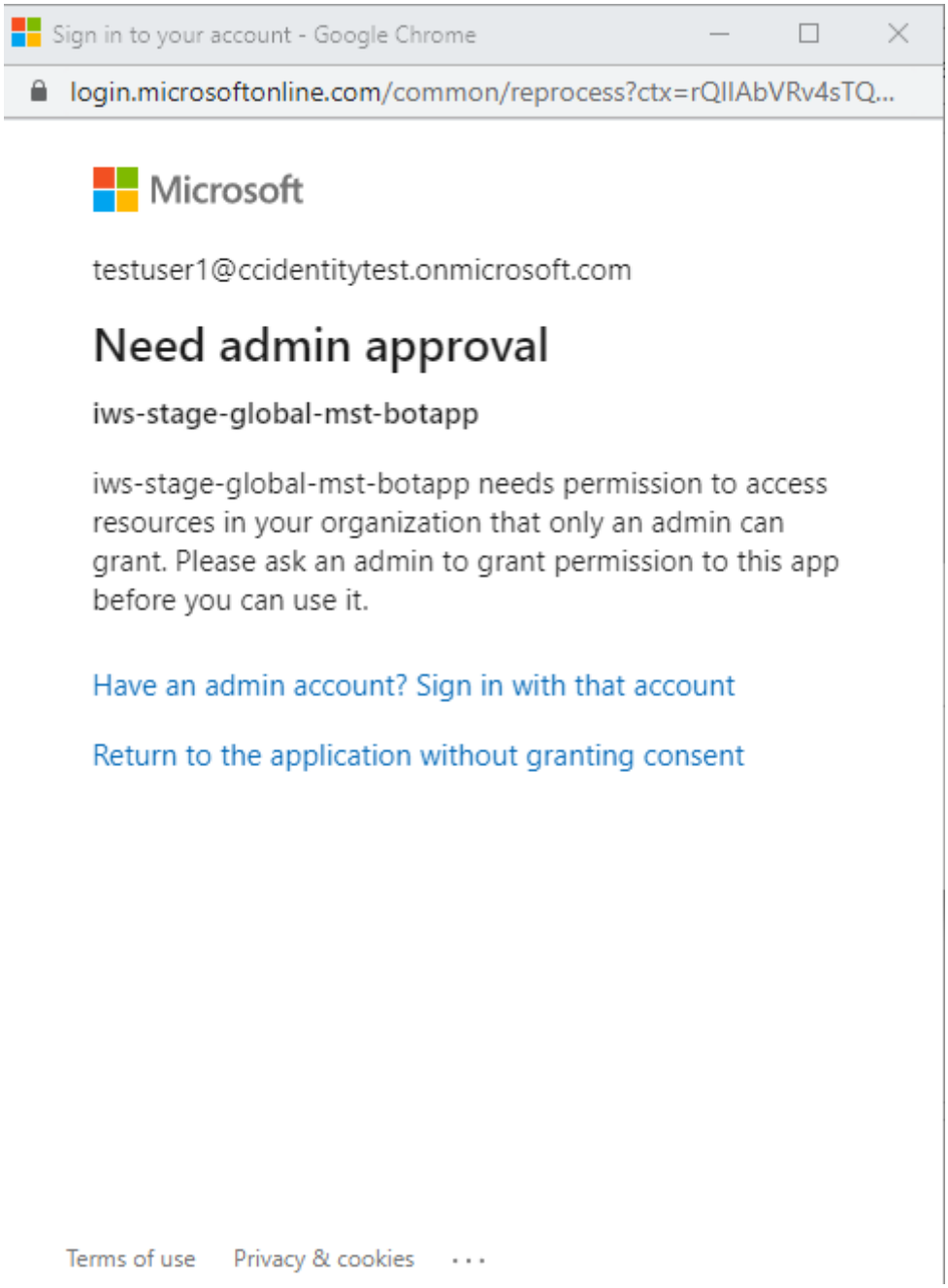
   Workspace users can now see the **Send to Microsoft Teams** option and share cards from Workspace. Users might need to refresh their screens (Ctrl+F5).



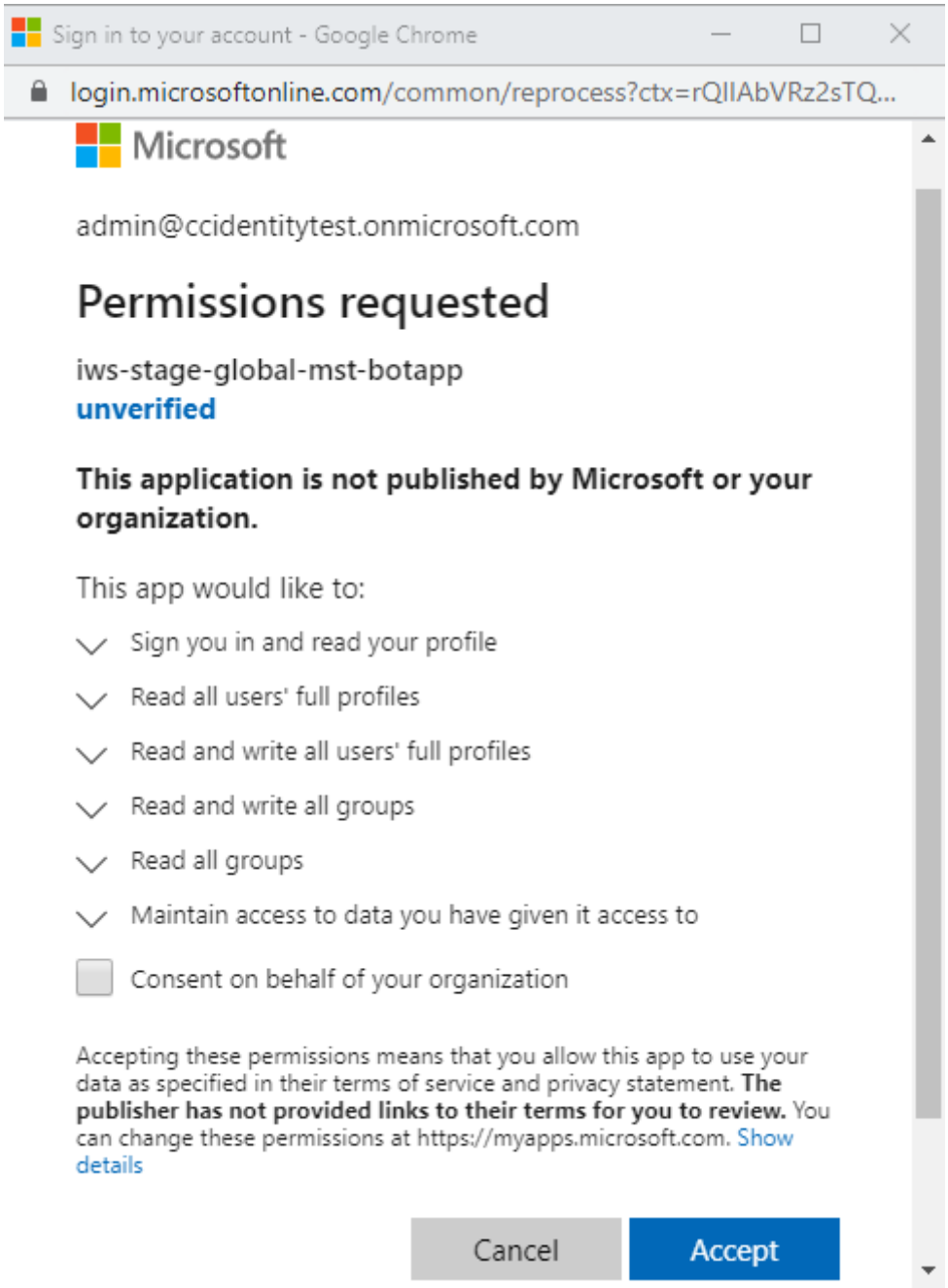
Accept Workspace permissions

There are other set-up steps that are required to enable this integration. The **Microsoft Administrator** account must accept the permissions of the integration in the Workspace UI so that users of your organization can share cards to Microsoft Teams.

1. Sign in to any workspace account and try to share a card.
2. The following message appears if the **Microsoft Administrator** account hasn't accepted permissions for integration with Microsoft Teams and you try to sign in with a non-administrator account:



3. To accept permissions, sign in to your administrator account by selecting **Have an admin account? Sign in with that account**. The following permissions to access data are required to enable the Microsoft Teams integration with Citrix Workspace:



4. When the **Permissions accepted** dialogue opens, review the options. The **Consent on behalf of your organization** grants permissions to all Workspace subscribers for this administrator. Otherwise, permissions are granted only for the administrator account.
5. Select **Accept**.

Customize security and privacy policies

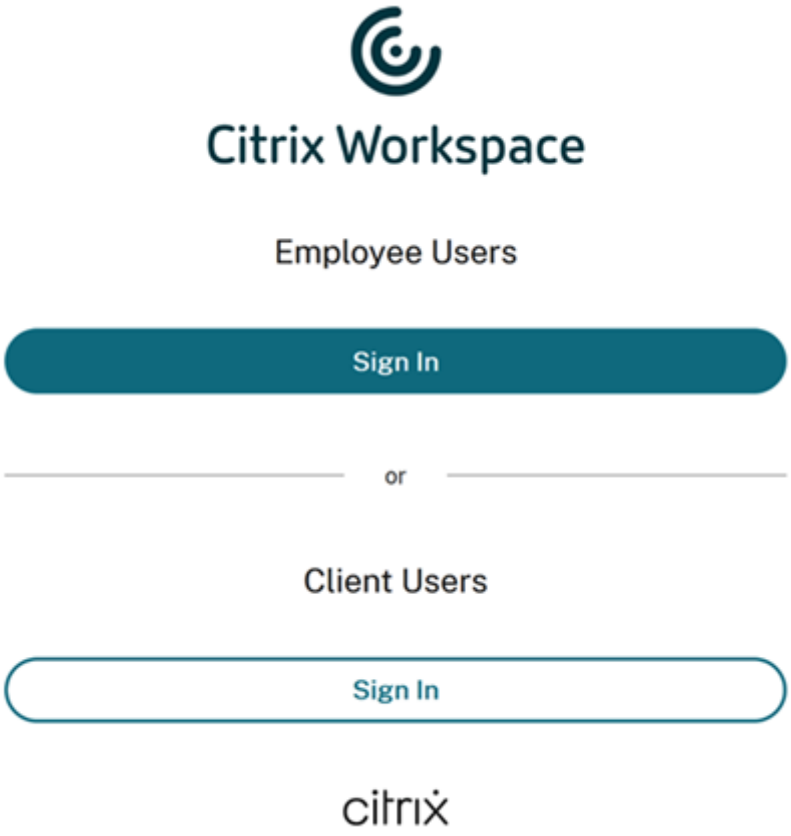
February 21, 2024

This article provides guidance on how to customize the sign-in experience after you've already configured workspace access and authentication.

For an overview on configuring workspace access and authentication, visit Configure access. For information on how to configure subscriber authentication to workspaces, visit Secure workspaces.

Create a unified user sign-in flow

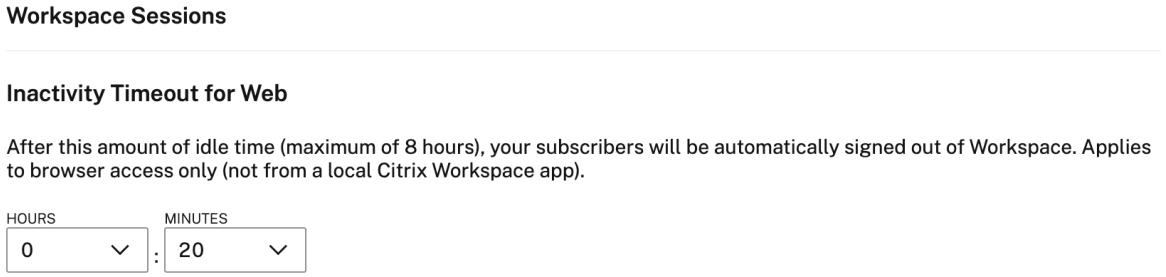
The default sign-in experience is a split screen for employee users and client (external) users.



To remove the split screen, navigate to **Workspace Configuration > Authentication > Unified user sign in flow** and select **Enable**. Enabling this feature presents all users with the same sign-in option.

Set inactivity timeout for Web and Workspace app desktop and mobile

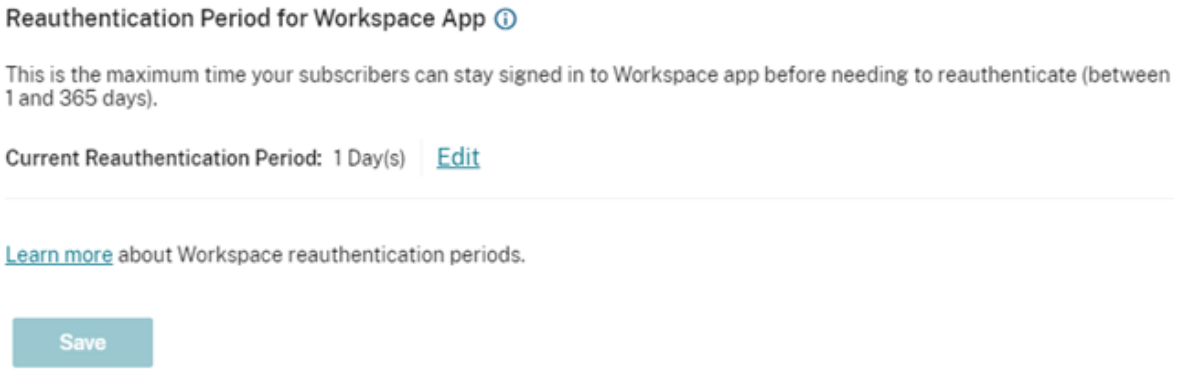
Use the **Inactivity Timeout for Web** setting in **Workspace Configuration > Customize > Preferences** to specify the amount of idle time allowed (a maximum of 8 hours) before subscribers are automatically signed out of Citrix Workspace. You can also enable inactivity timeout for the Workspace app on desktop and mobile by selecting the appropriate setting.



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

Set a reauthentication period for Citrix Workspace app

Use the **Reauthentication period for Workspace app** setting in **Workspace Configuration > Customize > Preferences** to specify the length of time subscribers can stay signed in to Citrix Workspace app before needing to sign in again.



By default, this setting requires subscribers to sign in every 24 hours (one day). You can specify a longer reauthentication period of up to 365 days. Longer reauthentication periods require subscriber consent to stay signed in. Users provisioned after September 27, 2021, a period of 30 days is required for subscribers to sign in again.

During the reauthentication period that you set, subscribers stay signed in unless they're inactive for 14 or more days at a time. If a subscriber is inactive for 14 or more days, they're prompted to reauthenticate the next time that they attempt to access their workspace.

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

If you need to set the reauthentication period for Citrix Workspace app to less than 24 hours, you can do so via PowerShell.
For more information, see Steps to configure InactivityTimeoutInMinutes.

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

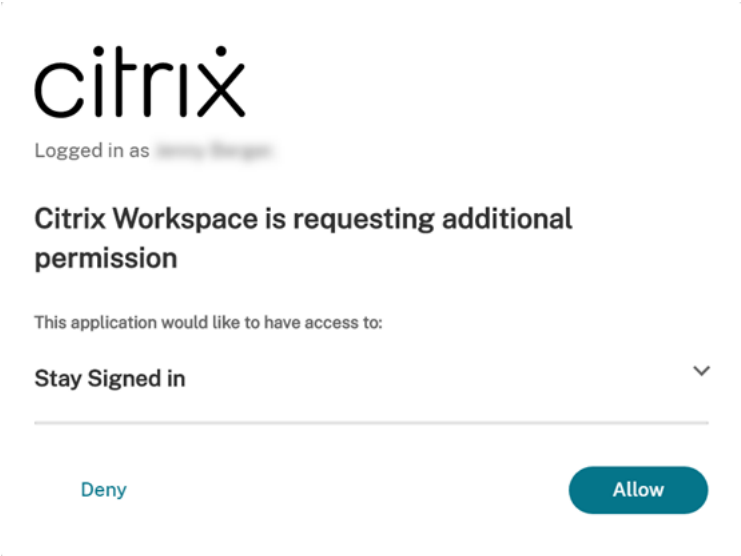
Staying signed in to Citrix Workspace app is supported for the following authentication methods:

- Active Directory
- Active Directory plus token
- Azure Active Directory
- 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 workspaces with Citrix Federated Authentication Service.

Subscriber experience for staying signed in

When subscribers sign in to Workspace on their device, Workspace prompts them to consent to staying signed in.



When the subscriber selects the **Allow** option, they stay signed in during the reauthentication period. If no activity is detected on a subscriber's device for four days, the subscriber is automatically prompted to reauthenticate. After they sign in to the Citrix Workspace app, the reauthentication period remains in effect as long as they're using their apps and desktops on the device.

If the subscriber selects **Deny**, Workspace prompts the subscriber to sign in again. Afterward, Workspace prompts the subscriber to sign in again after 24 hours have passed.

If the subscriber's password changes, the subscriber must sign out and sign in again through Citrix Workspace app for the reauthentication period to continue to work.

Allow subscribers to change their account password

> **Note:**
>
> This feature is being rolled out to customers incrementally. You might not be able to view the feature until the rollout process is complete.
>
> Citrix aims to deliver new features and product updates to Citrix Workspace customers when they're available. This process is transparent to you. Initial updates are applied to Citrix internal sites only, and are then applied to customer environments gradually. Delivering updates incrementally helps ensure product quality and maximize availability.

The **Allow Account Password to be Changed** setting in **Workspace Configuration > Customize > Preferences** controls whether subscribers can change their domain password from within Citrix Workspace. You can also provide guidance to subscribers so that they can create valid passwords in line with your organization's password policy.

When enabled (default), subscribers can change their password at any time, based on your organization's Active Directory settings. If disabled, Workspace prompts subscribers to change their password when it expires, but they can't change their unexpired password within Workspace.

Supported authentication methods

- Active Directory
- Active Directory plus token

Supported Workspace app clients

The following versions of Citrix Workspace app support this feature:

- Workspace app for Windows 2101 or later
- Workspace app for Mac 2012 or later
- Workspace app for Chrome 2010 or later
- Workspace app for HTML5 2101 or later
- Workspace app for Android 21.1.0 or later

Subscribers can also use this feature when accessing workspaces with the latest version of Edge, Chrome, Firefox, or Safari web browsers.

This feature isn't supported on the following:

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

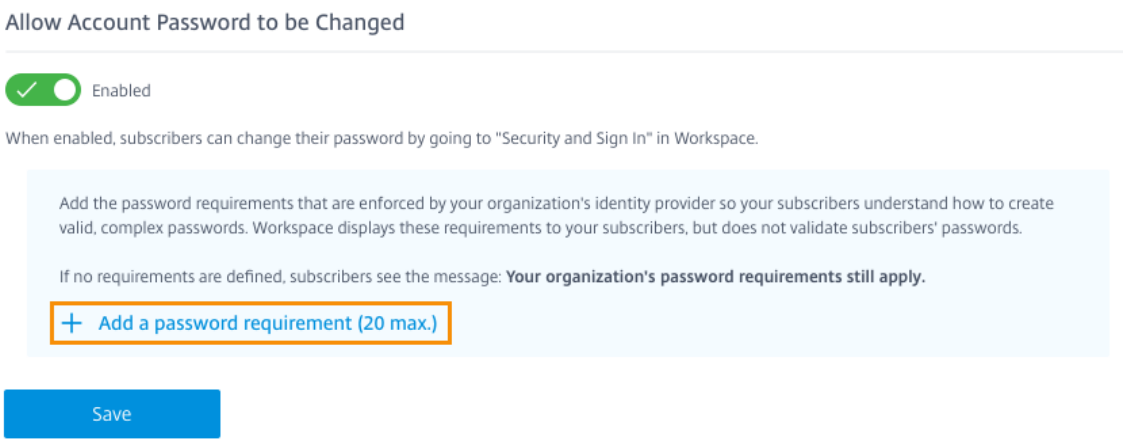
Password guidance

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

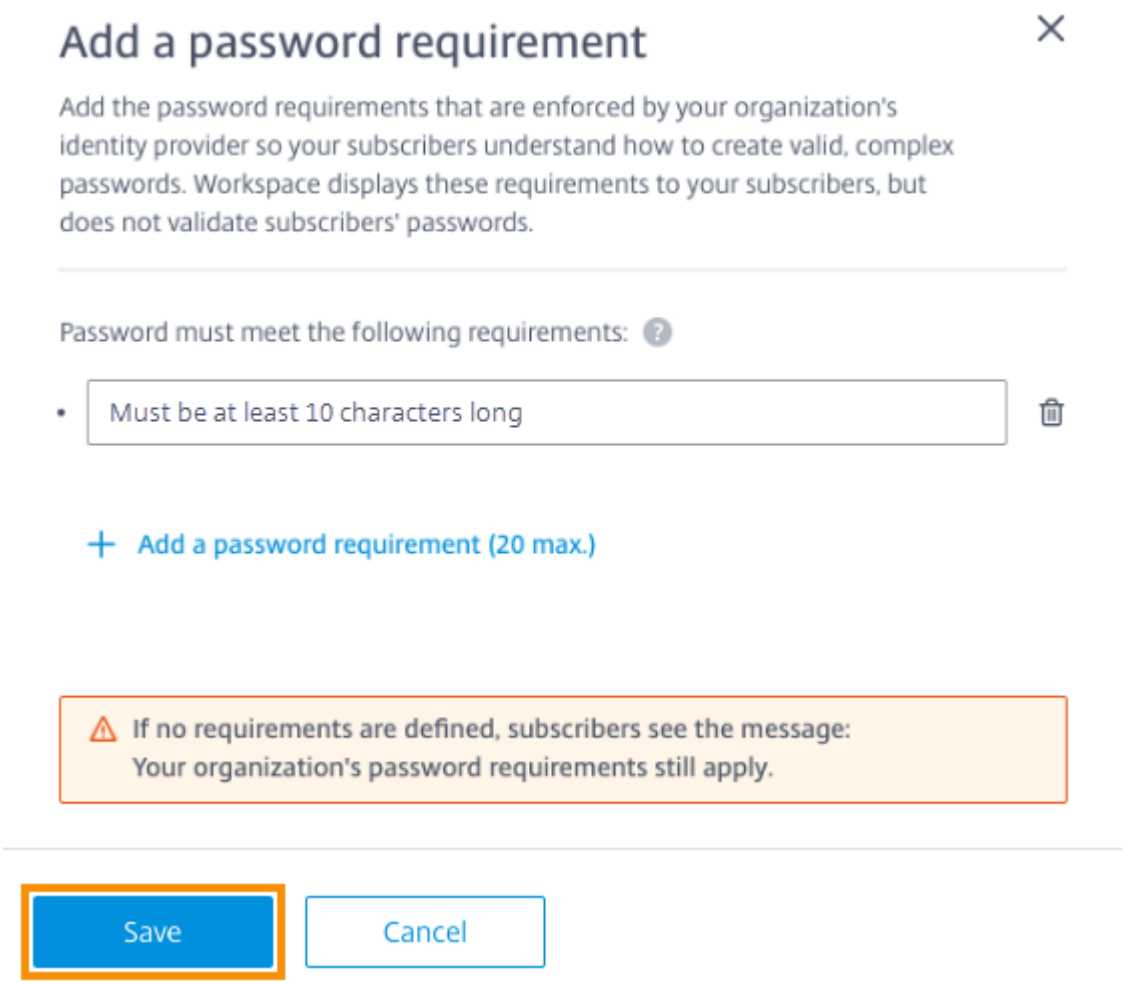
> **Important:**
>
> Citrix Workspace doesn't validate new passwords that your subscribers enter. If a subscriber tries to change their valid password to an invalid one through Workspace, your identity provider rejects the new password. The existing password isn't changed.

To add password requirements:

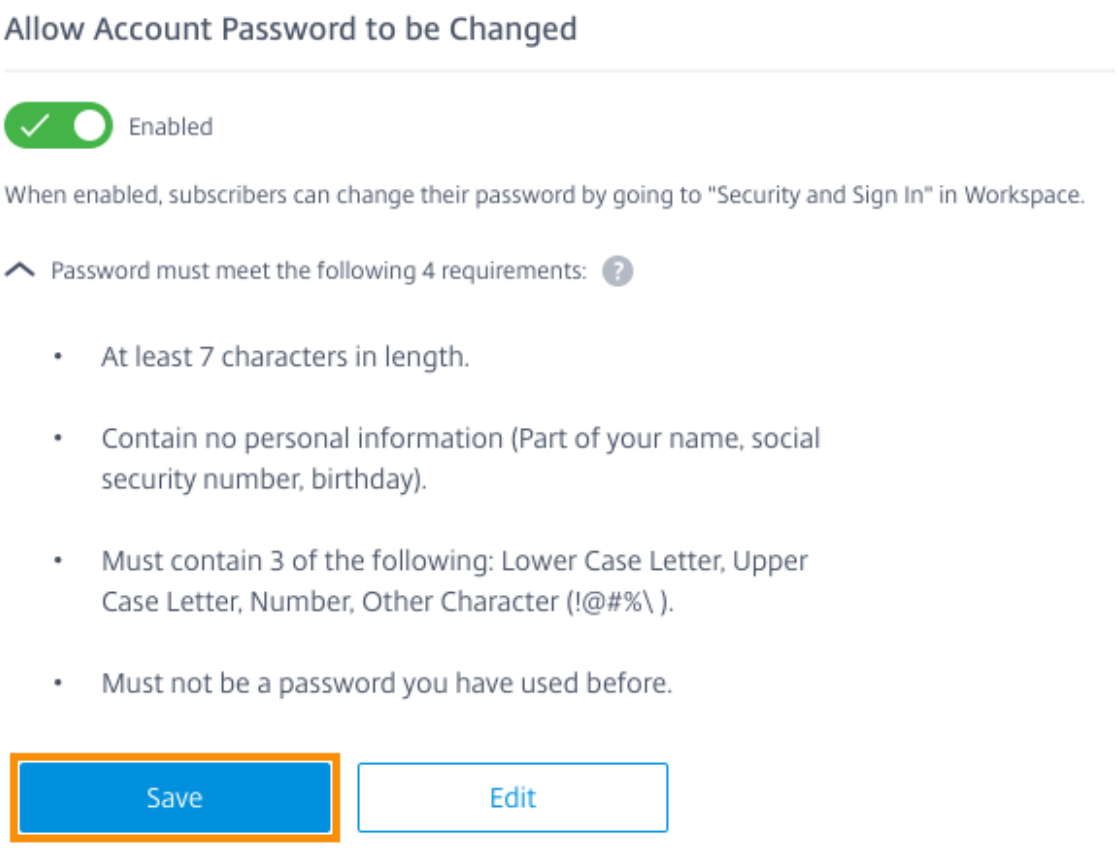
1. Navigate to **Workspace Configuration > Customize > Preferences**.
2. Under **Allow Account Password to be Changed**, check that the setting is in the enabled state. If disabled, enable the setting.
3. Select **Add a password requirement**.



4. 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 subscribers when they change their password.



5. When you're finished adding requirements, select **Save**.
6. Select **Save** again to save all your setting changes.

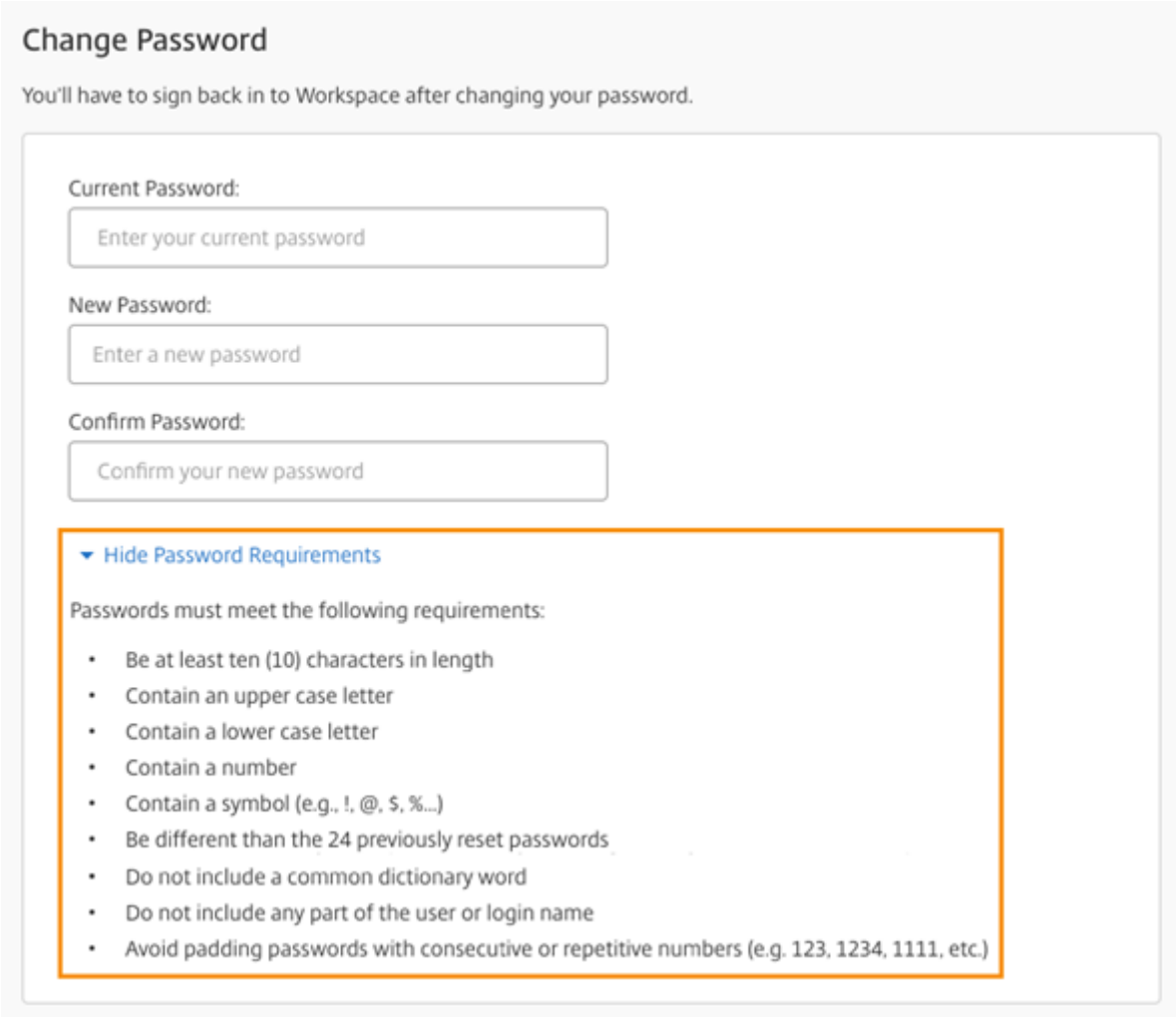


Subscriber experience when changing passwords

> **Tip:**
>
> To increase awareness of this feature with your subscribers, consider including a recommendation in your internal knowledgebase for subscribers to change their domain passwords through Workspace. Download pdf file for instructions you can include in your own communications and knowledgebase articles.

When **Allow Account Password to be Changed** is enabled, subscribers can change their password in Workspace by going to **Account Settings > Security & Sign in**.

Select **View Password Requirements** to display all the requirements you entered in **Workspace Configuration**.



Subscribers are automatically signed out of Workspace after changing their password and must sign in again with their new password.

Send custom announcements

Send a custom announcement to display a time-limited message of your choosing, such as an upcoming maintenance window.

The custom announcement is displayed for all subscribers in all clients including web and mobile devices. Subscribers see the message after they sign in. Subscribers can't dismiss this announcement, but they can minimize it on their mobile device.

1. From the **Citrix Cloud** menu, select **Workspace Configuration > Customize > Preferences > Send custom announcement > Configure**.
2. Enter the title and text of the message that you want to display, and select the dates, times, and placement (top or bottom) for displaying the message to subscribers.

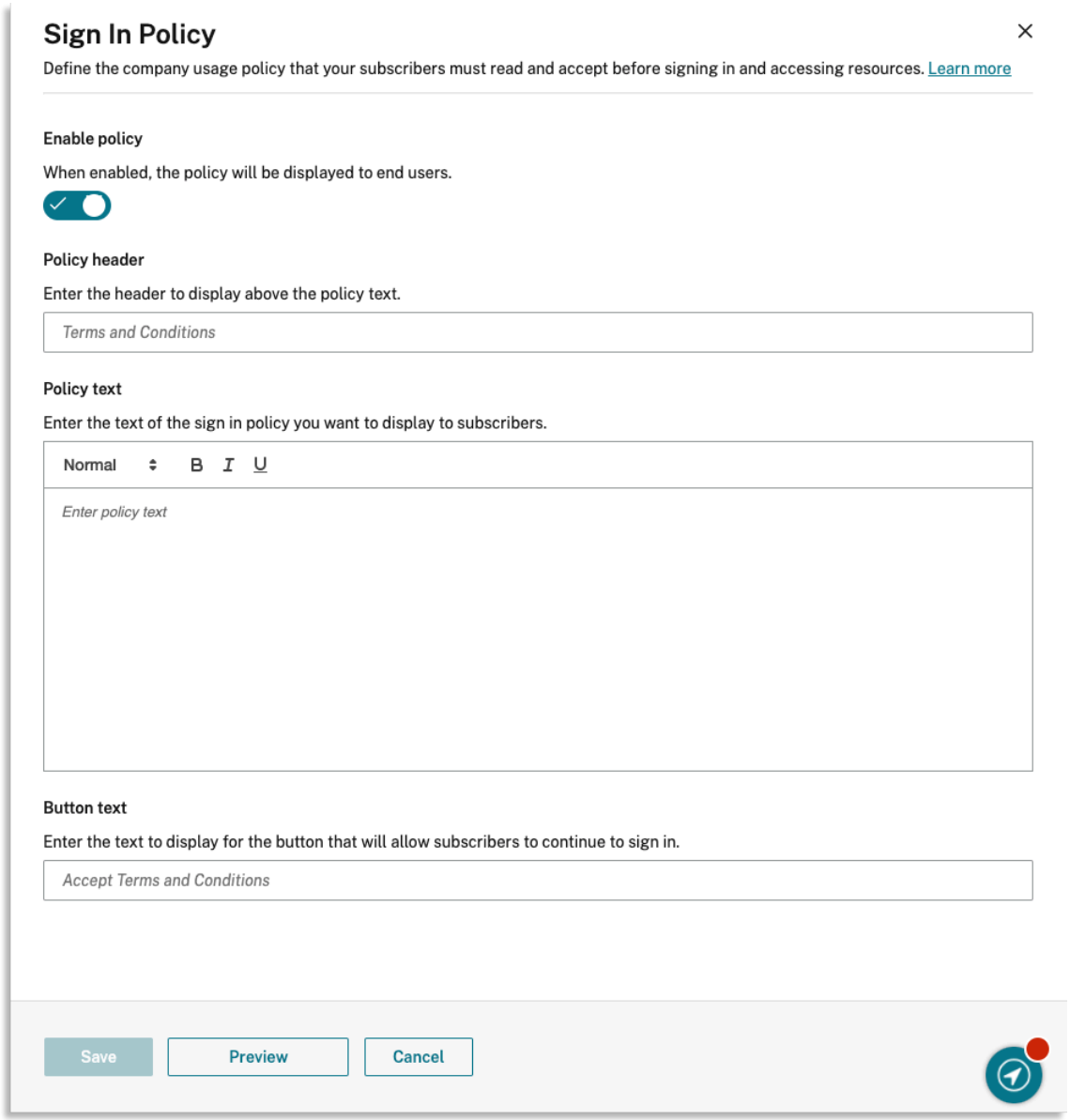
3. To view how your message appears to subscribers, select **Preview**.
4. When you're finished, select **Save**.

Configure a sign-in policy

Create a custom sign-in policy to inform subscribers of your organization's End-User License Agreement (EULA) when they sign in to their workspace.

When enabled and configured, the sign-in policy is displayed in all clients including web and mobile devices. Subscribers can see the sign-in policy when they sign in. Subscribers can't bypass the policy and must accept it to sign in to their workspace.

1. From the **Citrix Cloud** menu, select **Workspace Configuration > Customize > Preferences**.
2. In the **Sign in policy** section, select **Configure**. If a policy exists, the button reads **Edit**, instead.
3. Enable the feature using the toggle under **Enable policy**.
4. In **Policy header**, enter a title for the policy.
5. Enter the policy text that subscribers must agree to before signing in. If needed, add localized text for other languages in the same text box.
6. Enter a name for the button that subscribers must select to agree to the policy.



7. Select **Preview** to see what the policy looks like for subscribers.
8. When you're finished, select **Save**.

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

Optimize DaaS in Citrix Workspace

October 12, 2023

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 Workspace subscribers 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 Workspace so that subscribers can access these resources alongside cloud-managed resources.

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

For more information on scalability limits, see Workspace 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 subscribers 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 Workspace 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 Workspace supports using Citrix Federated Authentication Service (FAS) for single sign-on (SSO) to Citrix DaaS. FAS allows subscribers using a federated identity provider, such Azure AD or Okta, to enter their credentials only once when they sign in to their workspaces. Without FAS, subscribers using a federated identity provider are prompted to enter their credentials more than once to access their virtual apps and desktops.

Using FAS with Workspace 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 **Workspace Configuration**.

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

Aggregate Virtual Apps and Desktops in workspaces

February 16, 2024

You can add your site (Virtual Apps and Desktops deployment) to Citrix Workspace to make your existing apps and desktops available to subscribers. After adding your site, subscribers can access all their virtual apps and desktops alongside Files and other resources, when they sign in to their workspace. This process is known as *site aggregation*.

Site aggregation is available in all Citrix Workspace editions. For more information about the features included in each Workspace edition, see the Citrix Workspace Feature Matrix.

> **Note:**

> For information on aggregating DaaS sites, refer to Centralized site management (Technical Preview).

Aggregate on-premises Virtual Apps and Desktops

The following sections provide detailed information on aggregating on-premises Virtual Apps and Desktops.

Supported environments

Site aggregation is supported for on-premises deployments of the following Citrix products:

- Virtual Apps and Desktops 7 1808 or later
- XenApp and XenDesktop 7.0 through 7.18

On-premises sites running older versions of XenApp or XenApp and XenDesktop aren't supported for use with Citrix Workspace.

> **Important:**
>
> XenApp and XenDesktop 7.x includes versions that are End of Life (EoL). XenApp and XenDesktop releases before 7.14 reached EoL in June 30, 2018. Support for site aggregation with EoL versions of XenApp and XenDesktop 7.x depends on successful enumeration and launch of resources with your StoreFront deployment.

To use site aggregation with an on-premises deployment that includes the Citrix Federated Authentication Service (FAS), your site must use one of the following Citrix product versions:

- Virtual Apps and Desktops 7 1808 or later
- XenApp and XenDesktop 7.16 through 7.18

Connecting to Citrix Cloud is required for using FAS with Citrix Workspace. Update your FAS servers to the latest version of the FAS software so that you can connect to Citrix Cloud. For more information, see Enable single sign-on for workspaces with Citrix Federated Authentication Service.

Workspace platform scalability limits

The following scalability limits apply to Workspace platform:

Limit type	SLI metric	SLO threshold limit
Usage limits	Concurrent end users for all aggregated on-prem Citrix virtual apps and desktops sites	500
Extra backend/frontend integration limits	Number of on-prem Citrix virtual apps and desktops sites	4

> **Note:**
>
> If the number of backend/frontend integration sites increases beyond four, sites can experience slow response times. Service continuity or LHC support is also not present for on-prem sites.

Task overview

When you add your on-premises site to Citrix Workspace, the **Add Site** wizard guides you through the following tasks:

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.

The resource location specifies the domain and connectivity method for all users who access your site. During this process, Citrix Cloud tests connectivity to verify that your site is reachable from Cloud Connectors. Citrix Cloud then displays a list of your resource locations. If you have resource locations with no Cloud Connectors installed, download and install the required software.

For external connectivity, you can use your own Citrix Gateway or use the Citrix Gateway service. To only allow users on the same network as your site to access applications, specify internal-only access.

Prerequisites

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 Workspace.

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.

- Have no other Citrix components installed.
- Not be an Active Directory domain controller.
- Not be a machine that is critical to your resource location infrastructure.
- 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.
- Connect to the Internet. For more information, see System and Connectivity Requirements.

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

Site aggregation supports sites that use an on-premises Active Directory.

Azure Active Directory configuration To add sites using Azure Active Directory to Citrix Workspace, configure your site to trust XML Service requests. For detailed instructions, refer to the following articles:

For XenApp and XenDesktop 7.x and Virtual Apps and Desktops 7 1808, see CTX236929.

> **Important:**
>
> If you use Azure Active Directory, Okta, SAML, or other federated identity provider with workspaces and site aggregation, users are prompted to authenticate to each application they launch.
>
> FAS provides a single sign-on (SSO) experience for launching resources using federated authentication. To enable SSO for subscribers, register one or more FAS servers with the same resource location that you configured for adding your site.

Active Directory trusts 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 workspaces 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 Workspace support users from untrusted forests, these users can't use Citrix Workspace 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 Citrix Workspace. If users from an untrusted forest try to sign in to Citrix Workspace, they receive the error message, "Your logon has expired. Please log on again to continue."

Internal and external connectivity to workspace resources

During the process of adding your site to Citrix Workspace, 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 through Citrix Workspace, 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 Workspace. 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 Workspace, Citrix Cloud discovers your site and checks that the Controller you specify is available. Before you add your on-premises site, check the following:

- 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.

To enable site discovery without site credentials XenApp and XenDesktop 7.x and Virtual Apps and Desktops 7 1808 only: If you don't want to provide site credentials for security reasons, you can allow Citrix Cloud to discover your site without prompting for site credentials. Complete this task **before** you add your site to Citrix Workspace.

1. Install at least two Cloud Connectors in your site's domain.
2. Create an Active Directory security group and add the Cloud Connectors in your domain to it.
3. Restart the Cloud Connectors.
4. In Studio, grant the security group **Read Only** permissions, at a minimum.

Task 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 **Workspace Configuration > 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 Workspace. 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**

   > **Note:**
   >
   > If using an FQDN, you must have a DNS record that points to the Delivery Controller that you want to discover.
   >
   > For XenApp and XenDesktop 7.x sites, Citrix Cloud automatically discovers the XML server port.

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**.

Task 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 Citrix Workspace 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**.

Task 3: Configure connectivity

In this step, you specify whether you want to allow external or internal-only user access to your site through Citrix Workspace. 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**.

Task 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**.

Task 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. Subscribers can't see resources from the site until you enable it.

1. Navigate to **Workspace Configuration > Service Intergrations > Virtual Apps and Desktops On-Premises Sites** and select the ellipsis to open the site actions menu.
2. Enable the service integration so that subscribers can sign in to their workspaces 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 in Citrix Workspace with a rediscovery process.

1. Navigate to **Workspace Configuration > 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 Workspace, 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 **Workspace Configuration > 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 **Workspace Configuration > 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 Workspace.

1. Navigate to **Workspace Configuration > 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 Workspace, you can disable it. You can disable an individual on-premises site or all on-premises sites you've added to Citrix Workspace.

When sites are disabled, users can't access the on-premises applications in those sites through Citrix Workspace. 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.

To disable an on-premises site

1. Navigate to **Workspace Configuration > Sites**, select the ellipsis for the site you want to disable and then select **Disable**.
2. A confirmation message appears. Select **Disable** again.

To disable all on-premises sites

To disable all sites on the **Sites** page, disable the workspace service integration for all Virtual Apps and Desktops on-premises sites. For instructions, see To disable workspace integration for a service.

To re-enable an individual on-premises site or to add another site later on, you must first re-enable the workspace service integration for all sites on the **Service Integrations** page.

Delete a site from Citrix Workspace

If you no longer want your on-premises site configuration in Citrix Workspace, you can delete the site. When you delete a site, only the configuration for the site in Citrix Workspace is removed. Citrix Cloud doesn't change your site.

To delete a site, navigate to **Workspace Configuration > Sites**, select the ellipsis for the site you want to remove, and then select **Delete**.

Optimize connectivity to workspaces with Direct Workload Connection

November 15, 2023

With Direct Workload Connection in Citrix Cloud, you can optimize internal traffic to the apps and desktops in workspaces to make HDX sessions faster. Ordinarily, users on both internal and external networks connect to VDAs through an external gateway. This gateway might be on-premises in your organization or provided as a service from Citrix and added to the resource location within Citrix Cloud. Direct Workload Connection allows internal users to bypass the gateway and connect to the VDAs directly, reducing latency for internal network traffic.

To set up Direct Workload Connection, you need network locations that correspond to where clients launch apps and desktops in your environment. Add a public address for each office location where these clients reside using the Network Location Service (NLS). You have two options for configuring network locations:

- Using the **Network Locations** menu option in Citrix Cloud.
- Using a PowerShell module that Citrix provides.

Network locations correspond to the public IP ranges of the networks that your internal users connect from, such as your office or branch locations. Citrix Cloud uses public IP addresses to determine whether the networks from which virtual apps or desktops launched are internal or external to the company network. If a subscriber connects from the internal network, Citrix Cloud routes the connection directly to the VDA, bypassing NetScaler Gateway. If a subscriber connects externally, Citrix Cloud routes them through NetScaler Gateway, then directs the session traffic through the Citrix Cloud Connector to the VDA in the internal network. If the Citrix Gateway service is used and the Rendezvous protocol is enabled, Citrix Cloud routes external users through the Gateway service to the VDA in the internal network. Roaming clients such as laptops might use either of these network routes, depending on whether the client is inside or outside the corporate network when the launch occurs.

> **Important:**
>
> If your environment includes Citrix DaaS Standard for Azure alongside on-premises VDAs, configuring Direct Workload Connection causes launches from the internal network to fail.

Remote Browser Isolation, Citrix Virtual Apps Essentials, and Citrix Virtual Desktops Essentials resource launches always route through the gateway. These launches don't gain performance improvements from configuring Direct Workload Connection.

Requirements

Network requirements

- Corporate network and guest Wi-Fi networks must have separate public IP addresses. If your corporate and guest networks share public IP addresses, users on the guest network can't launch DaaS sessions.
- Use the public IP address ranges of the networks that your internal users connect from. Internal users on these networks must have a direct connection to the VDAs. Otherwise, launches of virtual resources fail as Workspace tries to route internal users directly to the VDA, which isn't possible.
- Although VDAs are typically located within your on-premises network, you can also use VDAs hosted within a public cloud such as Microsoft Azure. Client launches must have a network route to contact the VDAs without being blocked by a firewall. This requires a VPN tunnel from your on-premises network to a virtual network where the VDAs reside.

TLS requirements

TLS 1.2 must be enabled in PowerShell when configuring your network locations. To force PowerShell to use TLS 1.2, use the following command before using the PowerShell module:

```
[Net.ServicePointManager]::SecurityProtocol = [Net.SecurityProtocolType]::Tls12
```

Workspace requirements

- You have a workspace configured in Citrix Cloud.
- Citrix DaaS is enabled in **Workspace Configuration > Service Integrations**.

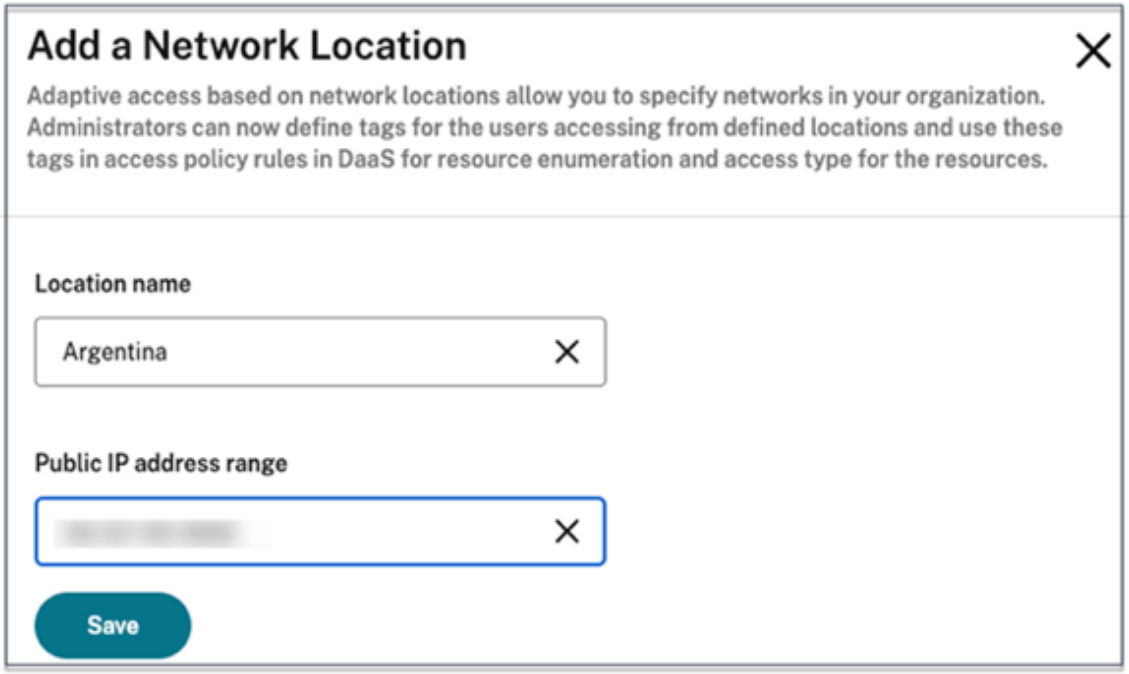
Enable TLS for Workspace app for HTML5 connections

If your subscribers use Citrix Workspace app for HTML5 to launch apps and desktops, Citrix recommends that you have TLS configured on the VDAs in your internal network. Configuring your VDAs to use TLS connections ensures direct launches to VDAs are possible. If VDAs don't have TLS enabled, app and desktop launches must be routed through a gateway when subscribers use Citrix Workspace app for HTML5. Launches using the Desktop Viewer aren't affected. For more information about securing direct VDA connections with TLS, see CTX134123 in the Citrix Support Knowledge Center.

Add network locations through the GUI

Direct Workload Connection configuration through Citrix Cloud involves creating network locations using the public IP address ranges of each branch location that your internal users connect from.

1. In the Citrix Cloud console, navigate to **Network Locations**.
2. Click **Add network location**.
3. Enter a network location name and public IP address range for the location.

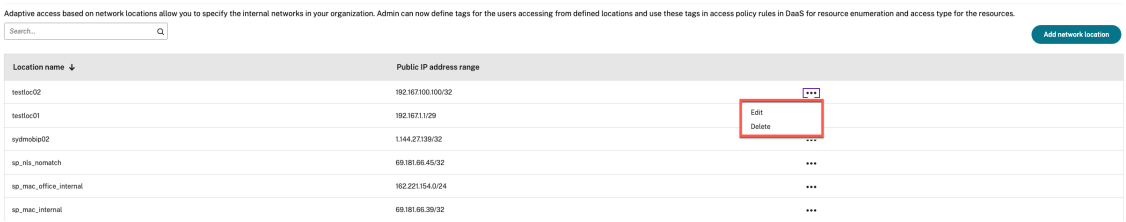


4. Click **Save**.
5. Repeat these steps for each new network location that you want to add.

> **Note:**
>
> Location tags are not required for Direct Workload Connection because the connectivity type is always **Internal**. The **Location tags** field in the **Add a Network Location** page (**Citrix Cloud > Network Locations > Add a Network Location > Location tags**) is only visible if the Adaptive Access feature is enabled. For details, see Enable the Adaptive Access feature.

Modify or remove network locations

1. In the Citrix Cloud console, navigate to **Network Locations** from the main menu.
2. Locate the network location that you want to manage and click the ellipses button.



3. Select one of the following commands:

   - Select **Edit** to modify the network location. After making changes, click **Save**.
   - Select **Delete** to remove the network location. Select **Yes, delete** to confirm the deletion. You can't undo this action.

Add and modify network locations with PowerShell

Instead of using the Citrix Cloud management console interface, you can use a PowerShell script to configure Direct Workload Connection. Direct Workload Connection configuration with PowerShell involves the following tasks:

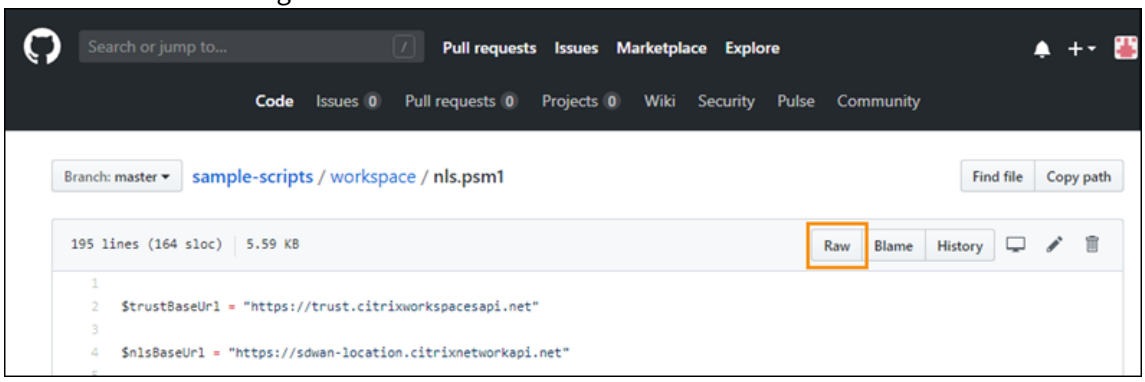
1. Determine the public IP address ranges of each branch location that your internal users connect from.
2. Download the PowerShell module.
3. Create a secure API client in Citrix Cloud and make a note of the Client ID and secret.
4. Import the PowerShell module and connect to the Network Location Service (NLS) with your API client details.
5. Create NLS sites for each of your branch locations with the public IP address ranges that you previously determined. Direct Workload Connection is automatically enabled for any launches that come from the internal network locations you've specified.
6. Launch an app or desktop from a device on your internal network and verify that the connection goes directly to the VDA, bypassing the Gateway. For more information, see ICA file logging in this article.

Download the PowerShell module

Before you set up your network locations, download the Citrix-provided PowerShell module (nls.psm1) from the Citrix GitHub repository. Using this module, you can set up as many network locations as needed for your VDAs.

1. In a web browser, go to https://github.com/citrix/sample-scripts/blob/master/workspace/NLS2.psm1.

2. Press **ALT** while clicking the **Raw** button.



3. Select a location on your computer and click **Save**.

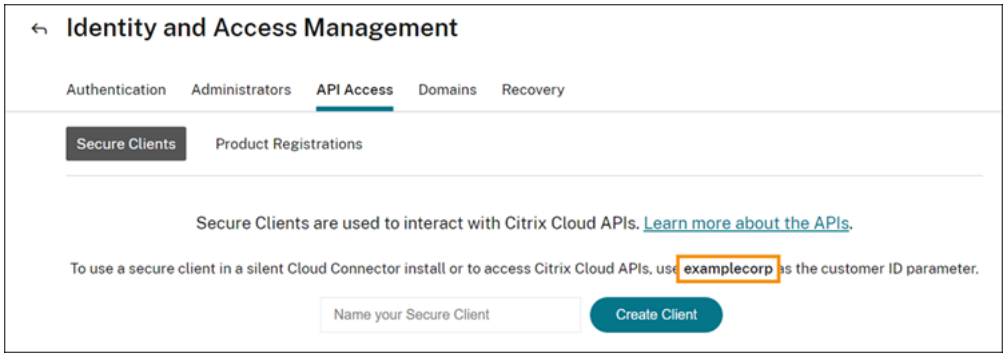
Required configuration details

To set up your network locations, you need the following required information:

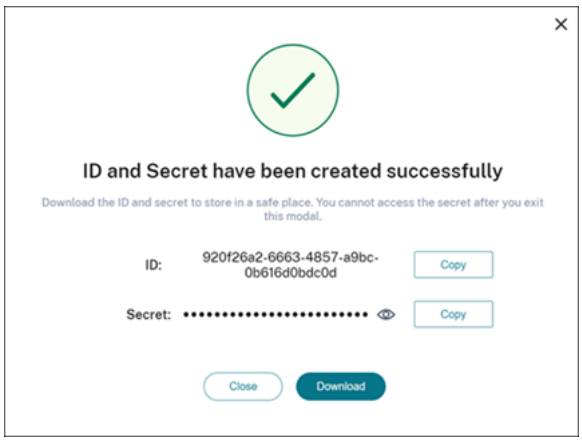
- Citrix Cloud secure client customer ID, client ID, and client secret. To obtain these values, see Create a secure client in this article.
- Public IP address ranges for the networks where your internal users are connecting from. For more information about these public IP address ranges, see Requirements in this article.

Create a secure client

1. Sign in to Citrix Cloud at `https://citrix.cloud.com`.
2. From the Citrix Cloud menu, select **Identity and Access Management** and then select **API Access**.
3. On the **Secure Clients** tab, note your customer ID.



4. Enter a name for the client and then select **Create Client**.
5. Copy the client ID and client secret.



Configure network locations

1. Open a PowerShell command window and navigate to the same directory where you saved the PowerShell module.
2. Import the module: `Import-Module .\nls.psm1 -Force`
3. Set the required variables with your secure client information from Create a secure client:
   - `$clientId = "YourSecureClientID"`
   - `$customer = "YourCustomerID"`
   - `$clientSecret = "YourSecureClientSecret"`
4. Connect to the Network Location Service with your secure client credentials:

```
Connect-NLS -clientId $clientId -clientSecret $clientSecret -
    customer $customer
```

5. Create a network location, replacing the parameter values with the values that correspond to the internal network where your internal users are directly connecting from:

```
New-NLSSite -name "YourSiteName" -tags @("YourTags") -ipv4Ranges @
    ("PublicIpsOfYourNetworkSites") -longitude 12.3456 -latitude
    12.3456 -internal $True
```

   To specify a single IP address instead of a range, add **/32** to the end of the IP address. For example:

```
New-NLSSite -name "YourSiteName" -tags @("YourTags") -ipv4Ranges @
    ("PublicIpOfYourNetworkSite/32") -longitude 12.3456 -latitude
    12.3456 -internal $True
```

> **Important:**
>
> When using the `New-NLSSite` command, include at least one value for each parameter. If

> you run this command without any command-line arguments, PowerShell prompts you to enter the appropriate values for each parameter, one at a time. The `internal` property is a mandatory Boolean property with possible values: `$True` or `$False` that maps to the UI via PowerShell. For example, `(UI)Network Internal -> (PowerShell)-internal=$True`.

When the network location is created successfully, the command window displays the details of the network location.

6. Repeat Step 5 for all your network locations where users are connecting from.
7. Run the command `Get-NLSSite` to return a list of all the sites you've configured with NLS and verify that their details are correct.

Modify network locations

To change an existing network location:

1. From a PowerShell command window, list all existing network locations: `Get-NLSSite`
2. To modify the IP range for a specific network location, type

   ```
   (Get-NLSSite)[N] | Set-NLSSite -ipv4Ranges @("1.2.3.4/32","4.3.2.1/32")
   ```

   where `[N]` is the number corresponding to the location in the list (starting with zero) and `"1.2.3.4/32","4.3.2.1/32"` are the comma-separated IP ranges you want to use. For example, to modify the first listed location, you type the following command:

   ```
   (Get-NLSSite)[0] | Set-NLSSite -ipv4Ranges @("98.0.0.1/32","141.43.0.0/24")
   ```

Remove network locations

To remove network locations that you no longer want to use:

1. From a PowerShell command window, list all existing network locations: `Get-NLSSite`
2. To remove all network locations, type `Get-NLSSite | Remove-NLSSite`
3. To remove specific network locations, type `(Get-NLSSite)[N] | Remove-NLSSite`, where `[N]` is the number corresponding to the location in the list. For example, to remove the first listed location, you type `(Get-NLSSite)[0] | Remove-NLSSite`.

Verify that internal launches are routed correctly

To verify that internal launches are accessing VDAs directly, use one of the following methods:

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

Citrix DaaS console

Select **Manage > Monitor** and then 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 To enable logging of the launch.ica file. After launching sessions, examine the **Address** and **SSLProxyHost** entries in the log 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
<!--NeedCopy-->
```

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
<!--NeedCopy-->
```

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
<!--NeedCopy-->
```

> **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.

Example script

The example script includes all commands that you might need to add, modify, and remove the public IP address ranges for your branch locations. However, you don't need to run all commands to perform any single function. For the script to run, always include the first 10 lines, from **Import-Module** through **Connect-NLS**. Afterward, you can include only the commands for the functions you want to perform.

```
Import-Module .\nls.psm1 -Force

$clientId = "XXXX" #Replace with your clientId
$clientSecret = "YYY"    #Replace with your clientSecret
$customer = "CCCCCC"  #Replace with your customerid

# Connect to Network Location Service
Connect-NLS -clientId $clientId -clientSecret $clientSecret -customer
    $customer

# Create a new Network Location Service Site (Replace with details
    corresponding to your branch locations)
New-NLSSite -name "New York" -tags @("EastCoast") -ipv4Ranges @("
    1.2.3.0/24") -longitude 40.7128 -latitude -74.0060 -internal $True

# Get the existing Network Location Service Sites (optional)
Get-NLSSite

# Update the IP Address ranges of your first Network Location Service
    Site (optional)
$s = (Get-NLSSite)[0]
$s.ipv4Ranges = @("1.2.3.4/32","4.3.2.1/32")
```



```
\$s | Set-NLSSite

# Remove all Network Location Service Sites (optional)
Get-NLSSite | Remove-NLSSite

# Remove your third site (optional)
\(Get-NLSSite)\[2] | Remove-NLSSite
```

Troubleshooting

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. For more information, see Requirements in this article.

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 workspace. 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. For more information, see Requirements in this article.

Errors when running PowerShell cmdlets on non-Windows platforms

If you experience errors when running cmdlets with the correct parameters on PowerShell Core, verify that the operation was carried out successfully. For example, if you experience errors when running the New-NLSSite cmdlet, run `Get-NLSSite` to verify that the site was created. Running these cmdlets on macOS or Linux platforms using PowerShell Core can result in an error even though the operation ran successfully.

If you experience this issue when running cmdlets with the correct parameters on a Windows platform using PowerShell, ensure you're using the latest version of the PowerShell module. With the latest version of the PowerShell module, this issue does not occur on Windows platforms.

Additional help and support

For troubleshooting help or questions, contact your Citrix sales representative or Citrix Support.

Service continuity

April 15, 2024

Service continuity removes or minimizes dependence on the availability of components involved in the connection process. Users can launch their Citrix DaaS apps and desktops regardless of the cloud services health status.

Service continuity allows users to connect to their DaaS apps and desktops during outages, as long as the user device maintains a network connection to a resource location. Users can connect to DaaS apps and desktops during outages in Citrix Cloud components or in public and private clouds. Users can connect directly to the resource location or through the Citrix Gateway Service.

Service continuity improves the visual representation of published resources during outages by using Progressive Web Apps service worker technology to cache resources in the user interface.

Service continuity uses Workspace connection leases to allow users to access apps and desktops during outages. Workspace connection leases are long-lived authorization tokens. Workspace connection lease files are securely cached on the user device. When a user signs in to Citrix Workspace, Workspace connection lease files are saved to the user profile for each resource published to the user. Service continuity lets users access apps and desktops during an outage even if the user has never launched an app or desktop before. Workspace connection lease files are signed and encrypted and are associated with the user and the user device. When service continuity is enabled, a Workspace connection lease allows users to access apps and desktops for seven days by default. You can configure Workspace connection leases to allow access for up to 30 days.

When users exit Citrix Workspace app, Citrix Workspace app closes but the Workspace connection leases are retained. Users exit the Citrix Workspace app by right-clicking its icon in the system tray or by restarting the user device. You can configure service continuity to delete or retain Workspace connection leases when users sign out of Citrix Workspace during an outage. By default, Workspace connection leases are deleted from user devices when users sign out during an outage.

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 Workspace 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 during an outage, users must sign in to Citrix Workspace before the outage occurs. When you enable service continuity, users must perform the following steps on their devices:

1. Download and install a supported version of Citrix Workspace app.
2. Add the Workspace URL for your organization to Citrix Workspace app (for example, `https://example.cloud.com`).
3. Sign in to Citrix Workspace.

When a user signs into Citrix Workspace for the first time, service continuity downloads Workspace connection leases to the user device.

Downloading Workspace 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.

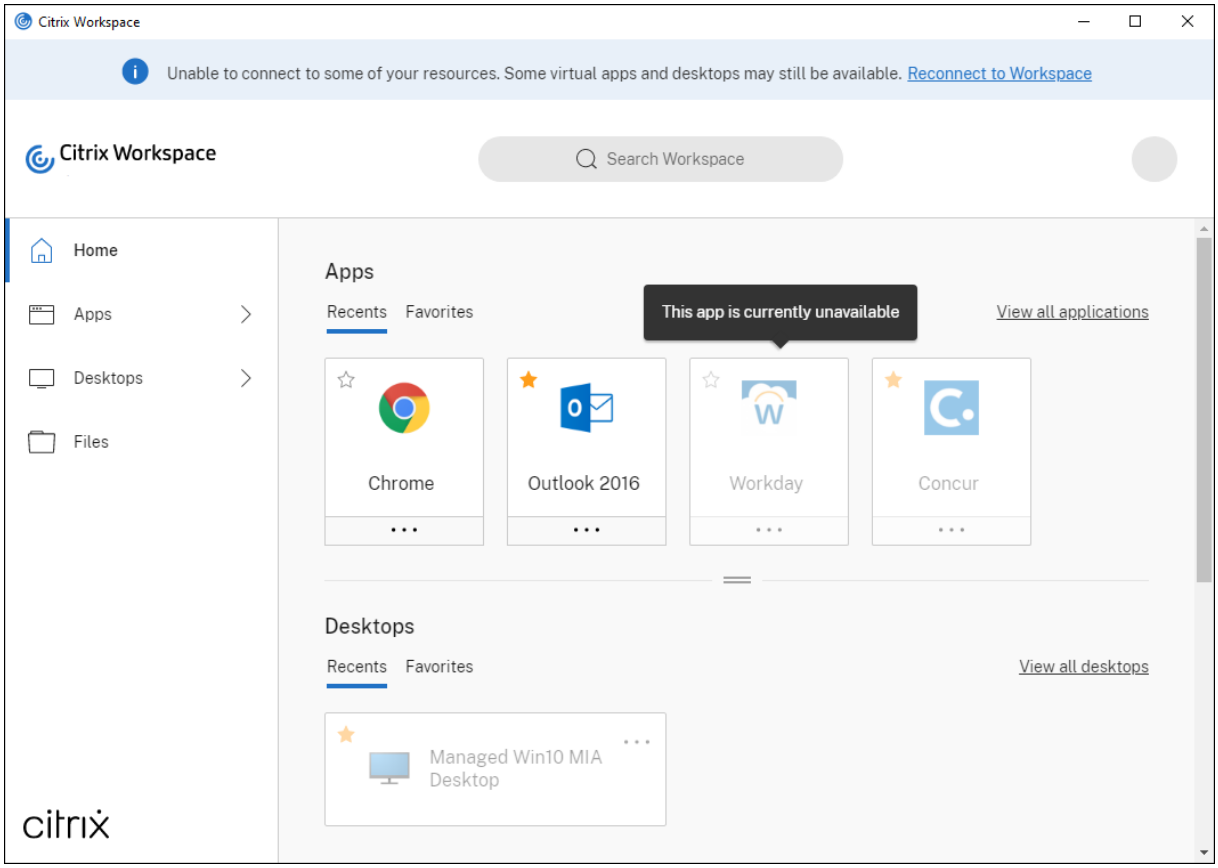
This table summarizes how service continuity helps users access apps and desktops during different types of outages.

Where the outage occurs	How service continuity maintains user access	User experience during outage
Citrix Workspace service	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 Workspace by clicking the "Reconnect to Workspace" link.
Identity provider	Citrix Workspace app and enumerates apps and desktops based on local cache on the user device.	Users might be unable to sign in to Workspace. Users click the "Use Workspace offline" link to access some apps and desktops in an experience identical to a Workspace service outage.
Citrix Cloud Broker Service	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.	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	Workspace 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.

Where the outage occurs	How service continuity maintains user access	User experience during outage
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 Workspace by clicking the "Reconnect to Workspace"link.

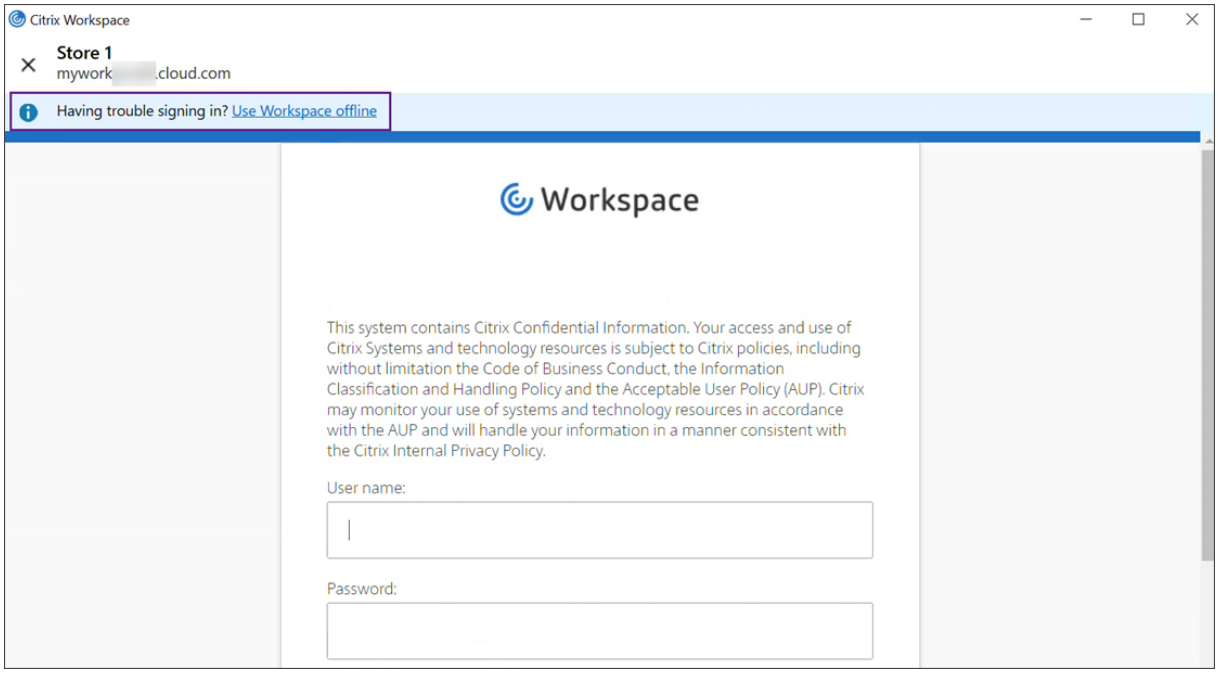
For information about validating outage scenarios in a non-production environment, refer to the Service Continuity Companion Guide.

During a Citrix Workspace outage, users see this message at the top of the Citrix Workspace 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. If prompted, the user then reenters their AD credentials at the VDA before accessing resources.

During an outage in the identity provider for workspace authentication, users might be unable to sign in to Citrix Workspace through the Workspace sign-in page. After 40 seconds, this message appears at the top of the Citrix Workspace home page.



Afterward, the Citrix Workspace home page appears. Users then access resources as they would during a Citrix Workspace outage.

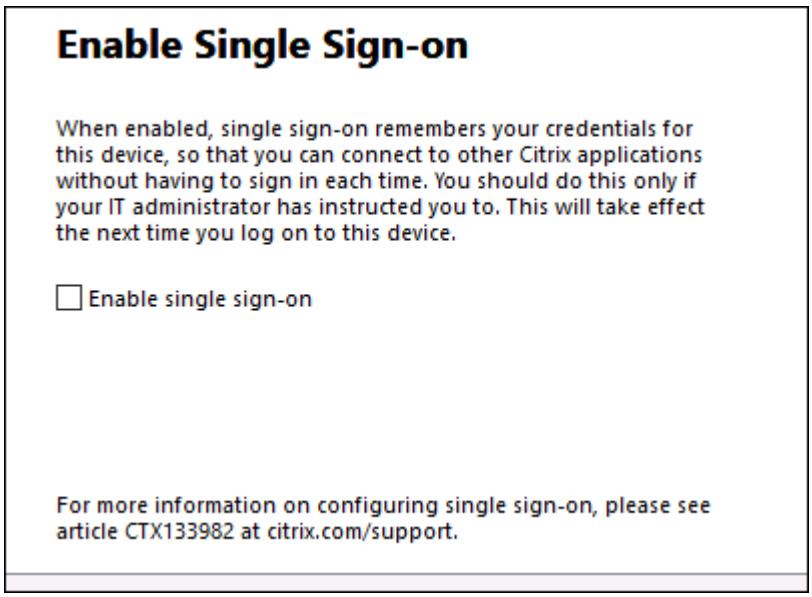
Regardless of the type of outage, users can continue to access resources if they exit and relaunch Citrix Workspace app. Users can restart their user devices without losing access to resources.

In the default configuration of service continuity, users lose access to their resources if they sign out of Citrix Workspace. If you want users to retain access to their resources after signing out, specify that Workspace connection leases are kept when users sign out. See Configure service continuity.

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. This step is required when user credentials aren't passed through during outages. Before accessing an app or desktop, users must reauthenticate to the VDA.

Users can access resources without entering their AD credentials if:

- Citrix Workspace is configured for single sign-on during installation by selecting the single sign-on box.



- Citrix Workspace app is configured with domain pass-through authentication. Users can access any available resource during a Citrix Workspace outage without entering their credentials. For information about configuring domain pass-through authentication for Citrix Workspace app for Windows, see Configure single sign-on using the graphical user interface, found in the **Authenticate** documentation.

  > **Note**
  >
  > StoreFront isn't needed to allow single sign-on to your VDA during an outage.

- 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.

Requirements and limitations

Site requirements

- Supported in all editions of Citrix DaaS and Citrix DaaS Standard for Azure, when using Workspace Experience.
- Not supported for Citrix Workspace 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 as a Workspace 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

> **Note:**
>
> For information on installing Citrix Workspace app for Linux, including information about installing the app for use with service continuity, see Citrix Workspace app for Linux.

- For users who access their apps and desktops using browsers:
  - Google Chrome or Microsoft Edge.
  - 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 Mac version 2206 at a minimum for use with Safari browser.

  See Service continuity in browser.
- Only one user per device is supported. Kiosk or "hot desk" user devices aren't supported.

Supported workspace authentication methods

- Active Directory
- Active Directory plus token
- Azure Active Directory
- Okta
- Citrix Gateway (primary user claim must be from AD)
- SAML 2.0

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 isn't supported.
- Local mapped accounts aren't supported.
- VDAs joined to Azure AD aren't supported. All VDAs must be joined to an AD domain.

Citrix Cloud Connector scale and size

- 4 vCPU or more
- 4 GB memory or more

Citrix Cloud Connector Powershell Security

Make sure script execution is enabled by setting the Execution Policy to **remotedSigned** value appropriate for your environment.
Other script execution privileges can also work, like **Default** or **AllSigned**.

Citrix Cloud Connector connectivity

Citrix Cloud Connector must be able to reach `https://rootoftrust.apps.cloud.com`. Configure your firewall to allow this connection. For information about the Cloud Connector firewall, see Cloud Connector Proxy and Firewall Configuration.

Workspace app network connectivity

If you configure connection to your resource location from outside your LAN, the Workspace app on user devices must be able to reach the Citrix Gateway Service FQDN, `https://*.g.nssvc.net`. Ensure that your firewall is configured to allow outgoing traffic to `https://global-s.g.nssvc.net:443`, so that user devices can connect to the Citrix Gateway Service at all times.

Connectivity optimization limitations

Advanced Endpoint Analysis (EPA) isn't supported.

Enlightened Data Transport (EDT) isn't supported during outages.

VDA requirements and limitations

- VDA 7.15 LTSR or any current release that hasn't reached end of life are supported.
- VDAs joined to Azure AD aren't supported. All VDAs must be joined to an AD domain.
- VDAs must be online for users to access VDA resources during an outage. VDA resources aren't available when the VDA is affected by outages in:
  - AWS
  - Azure
  - Cloud Delivery Controller, unless Autoscale is enabled for the delivery group delivering the resource
- VDA 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 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 **Workspace Configuration > 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 **Workspace Configuration > Access**.
2. Select **Configure Connectivity**.
3. Select **Gateway Service** as your connectivity type.
4. Click **Save**.

Configure for connections both from outside and inside your LAN

Run this PowerShell command:

```
Set-ConfigZone -InputObject (get-configzone -ExternalUid YourResourceLocationE
)-EnableHybridConnectivityForResourceLeases $true
```

Replace `YourResourceLocationExternalUid` with the external UID of the resource location.

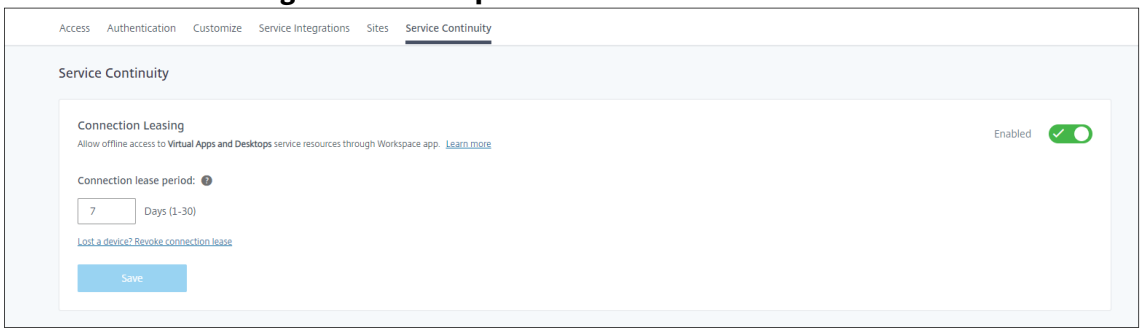
This command allows direct connections to the Citrix Cloud Connector FQDN over TCP 2598 during outages. If that connection fails Gateway Service is used as fallback. Allow internal users to bypass the gateway and connect directly to the resource location reduces latency internal network traffic.

> **Note:**
>
> This PowerShell command is similar to Direct Workload Connection in that it optimizes connectivity to workspaces by allowing internal users to bypass the gateway and connect to VDAs directly. When service continuity is enabled, Direct Workload Connection is not available during outages.

Configure service continuity

To enable service continuity for your site:

1. From the Citrix Cloud menu, go to **Workspace Configuration > Service continutity**.
2. Set **Connection leasing for the Workspace** to **Enable**.



3. Set **Connection lease period** to the number of days a Workspace connection lease can be used to maintain a connection. The Workspace connection lease period applies to all Workspace connection leases through your site. The Workspace connection lease period starts the first time a user signs in to the Citrix Cloud Workspace store. Workspace connection leases are refreshed each time the user signs in, up to once a day. The Workspace 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, Workspace connection leases are deleted from the user device if the user signs out of Citrix Workspace during an outage. If you want Workspace connection leases to remain on user devices after users sign out, use the following PowerShell command:

```
Set-BrokerSite -DeleteResourceLeasesOnLogOff $false
```


> **Note:**
>
> Workspace connection leases can't be set to remain on user devices after users sign out for users connecting with Citrix Workspace app for Mac. Citrix Workspace for Mac is unable to read the value of the `DeleteResourceLeaseOnLogOff` property.

How service continuity works

If there's no outage, users access virtual apps and desktops using ICA files. Citrix Workspace 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 Workspace to access resources. When service continuity isn't enabled, outages can prevent users from accessing resources if Citrix Workspace can't generate an ICA file.

Citrix Workspace generates ICA files when users launch virtual apps and desktops regardless of whether service continuity is enabled. When service continuity is enabled, Citrix Workspace also generates the unique set of files that make up a Workspace connection lease. Unlike ICA files, Workspace connection lease files are generated when the user signs into Citrix Workspace, not when the user launches the resource. When a user signs in to Citrix Workspace, connection lease files are generated for every resource published to that user. Workspace connection leases contain information that gives the user access to virtual resources. If an outage prevents a user from signing in to Citrix Workspace or accessing resources using an ICA file, the connection lease provides authorized access to the resource.

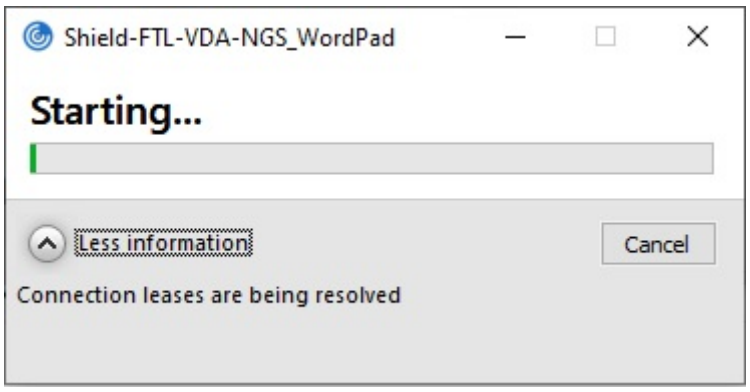
How sessions launch during outages

When users click an icon for an app or desktop during an outage, the Citrix Workspace app finds the corresponding Workspace 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.

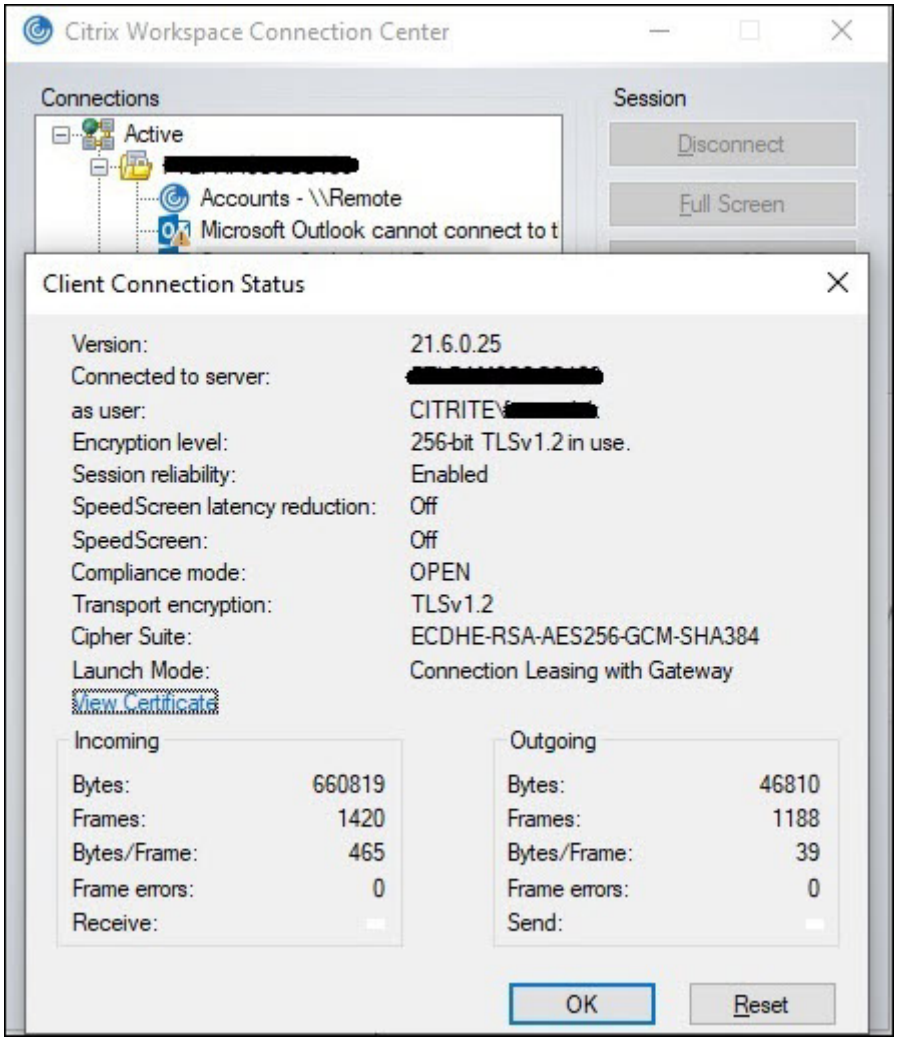
When the Citrix Cloud broker is online, the Cloud Connector uses the Citrix Cloud broker to resolve which VDA is available. When the Citrix Cloud broker is offline, the secondary broker for the Cloud Connector (also known as the High Availability service) listens for and processes connection requests.

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 Workspace connection leases were used for the session launch:



After the user has finished signing into the session, these properties appear in the Workspace Connection Center:



The launch mode property provides information about the Workspace connection leases used to

launch the session.

On devices running Citrix Workspace app for Mac, Citrix Viewer displays information showing that Workspace connection leases were used for the session launch:

What makes it secure

All sensitive information in the Workspace connection lease files is encrypted with the AES-256 cipher. Workspace 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.

Workspace 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 Workspace connection leases. When you block Workspace connection leases associated with a user, the user can't connect to resources. Citrix Cloud no longer generates or synchronizes Workspace connection leases for the user.

When you block Workspace connection leases associated with a user account, you block connections to that account on all devices associated with it. You can block Workspace connection leases for a user or for all users in a user group.

To revoke Workspace 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:

```
1 Set-BrokerConnectionLeaseRevocationDate -Name xd.local/user1 -
     LeaseRevocationDays 7
```

To view the time period for which Workspace 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 Workspace connection leases are revoked for xd.local/user1, type:

```
1 Get-BrokerConnectionLeaseRevocationDate -Name xd.local/user2
```

This information appears:

```
1 FullName                          :
2 Name                              : XD\user2
3 UPN                               :
4 Sid                               : S-1-5-21-nnnnnn
5 LeaseRevocationDays               : 2
6 LeaseRevocationDateTimeInUtc      : 2020-12-17T17:34:25Z
7 LastUpdateDateTimeInUtc           : 2020-12-19T17:34:25Z
```

From this output, you can see that user xd.local/user2 has Workspace 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 Workspace 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 Citrix Workspace 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 Workspace connection leases. When a user signs in to Citrix Workspace on a physical device, Workspace 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 Citrix Workspace on the virtual desktop. At this point, a different set of Workspace connection leases is downloaded and saved the user profile on the virtual desktop. Workspace connection lease files are associated with the device they're downloaded to. Workspace 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, Workspace 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

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.

Power management of VDAs during outages

If Cloud Connectors lose connectivity to Citrix Cloud, Connectors are unable to 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 Workspace connection lease.

Monitoring and troubleshooting

Service continuity performs two main actions:

- Download Workspace connection leases to the user device. Workspace connection leases are generated and synced with the Citrix Workspace app.
- Launch virtual desktops and apps using Workspace connection leases.

Troubleshooting downloading Workspace connection leases

You can view Workspace 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 Workspace 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`

Workspace connection leases are generated when the Citrix Workspace app connects to the Workspace store. View registry key values on the user device to determine whether the Citrix Workspace app has successfully contacted the Workspace 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 Workspace connection lease service:

- `leaseLastCallHomeTime`
- `leaseLastSyncStatus`

If the Citrix Workspace app tried unsuccessfully to contact the Workspace connection lease service, `leaseLastCallHomeTime` 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 Workspace 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 Workspace 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 Workspace.
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`.

Service continuity in browser

Extensions for Google Chrome and Microsoft Edge make service continuity available to Windows users who access their apps and desktops using those browsers. The extensions are called a Citrix Workspace Web extension and are available at the Chrome web store and the Microsoft Edge Add-on website.

These browser extensions require a native Citrix Workspace app on the user device to support service continuity. These versions are supported:

- 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. Supported with Google Chrome.
- Citrix Workspace app for Mac version 2206 at a minimum for use with Safari browser.

Citrix Workspace app for Windows (Store) is not supported.

The native Workspace app communicates with the Citrix Workspace Web extension using the native messaging host protocol for browser extensions. Together, the native Workspace app and the Workspace Web extension use Workspace connection leases to give browser users access to their apps and desktops during outages.

This video shows how to install and use service continuity in browser.

This is an embedded video. Click the link to watch the video

User device setup for browser users

To use service continuity in a browser, users must perform the following steps on their devices:

1. Download and install a version of Citrix Workspace app that is supported for browser users.
2. Download and install the Citrix Workspace Web extension for Chrome or Edge.

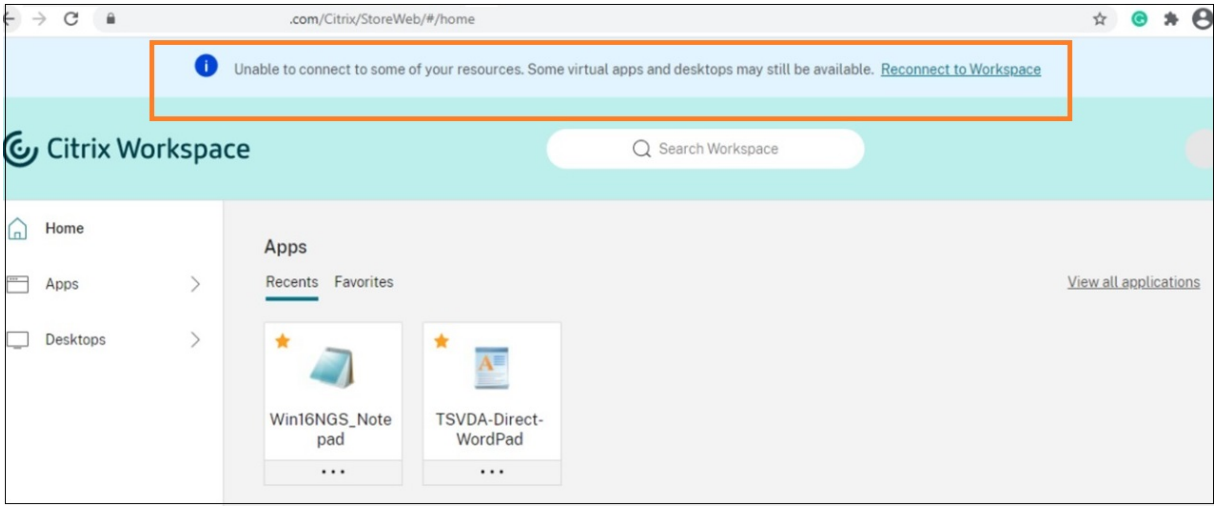
Browser user experience

When users click their apps or desktops, the app or desktop opens without users being prompted to open the **Citrix Workspace launcher**.

Browser user experience during outages

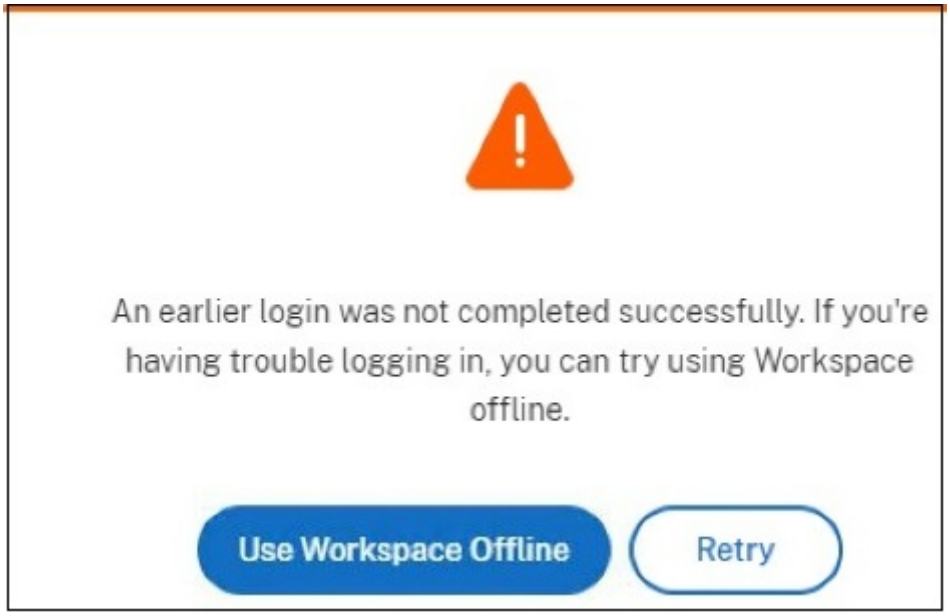
Users can access their apps and desktops from a browser during outages, as long as the user device maintains a network connection to a resource location.

If an outage occurs while the user is logged in to Workspace through a browser, this message appears near the top of the browser window:



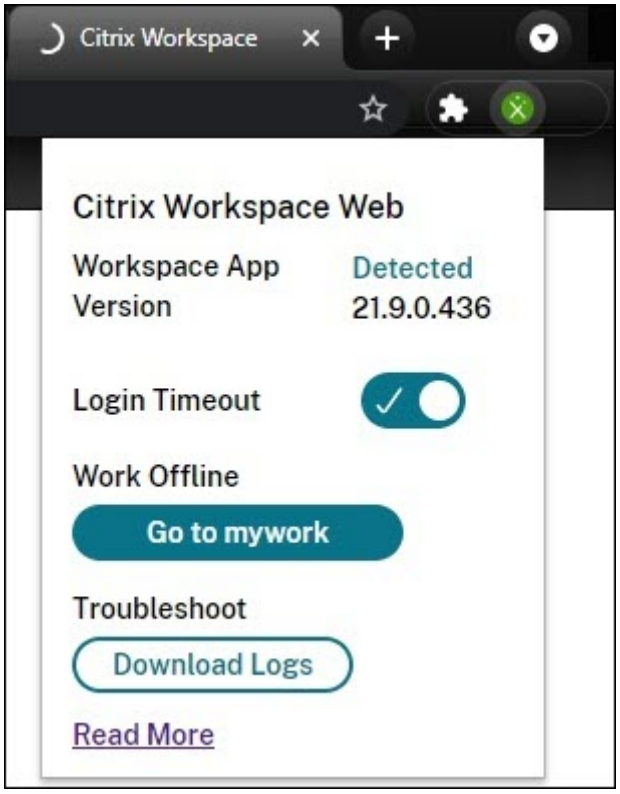
Users can access apps and desktops that are available offline by clicking any icon that is not dimmed. Users can also try to get back online by clicking **Reconnect to Workspace**.

When an outage prevents users from logging in to Workspace through a browser, the user is prompted work offline or try logging in again. To access available apps and desktops offline, users click **Use Workspace Offline**.



If an outage prevents users from logging in to the Workspace after navigating to the Workspace URL, the window appears after a specified timeout interval. By default, the window appears 30 seconds after the user navigates to the Workspace URL. You can set this value to 15, 30, 45 or 60 seconds. You can also disable the login timeout. If the login timeout is disabled, the window prompting users to work offline appears when the user navigates to the Workspace URL.

To configure the login timeout setting, click the extension icon in the browser on the user device. Use the window that appears to enable or disable login timeout and set the timeout duration:



An outage might prevent the user from logging in if the browser has been redirected to a third-party identity provider authentication site. In this case, the user can type the Workspace URL into the browser, which causes the window prompting users to work offline to appear. The user doesn't have to wait through the login timeout interval for the window to appears.

Users can also access apps and desktops available during an outage this way:

1. Click the extension icon in the browser.
2. In the window that appears, click the button under **Work Offline**. This button says **Go to** and then the name of your Workspace store.
3. In the window that appears, click **Use Workspace Offline**.

During some outages, the warning window prompting users to work offline appears automatically when the extension detects Workspace-side issues. The user doesn't need to take any action or wait through the login timeout interval.

Browser limitations

If users clear cookies and other site data in their browsers during an outage, service continuity doesn't work until they authenticate to Workspace again.

Unless the user enables the extension to work in incognito mode, service continuity isn't supported in incognito mode.

Troubleshooting for browser users

In the **Advanced** menu of the Citrix Workspace browser app account settings, ensure the current method for app and desktop launch preference is set to **Use Citix 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 Workspace URL.

To download logs, click the extension icon in the browser. Then click **Download Logs**.

Enable single sign-on for workspaces with Citrix Federated Authentication Service

November 27, 2023

Citrix Federated Authentication Service (FAS) supports single sign-on (SSO) to DaaS in Citrix Workspace. FAS is typically adopted if you're using one of the following identity providers for Citrix Workspace authentication:

- Azure Active Directory
- Okta
- SAML 2.0
- Citrix Gateway
- Google Cloud Identity

With FAS, subscribers enter their credentials only once to access their DaaS apps and desktops.

FAS isn't needed for SSO to DaaS 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.

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, subscribers signing in to their workspaces through a federated identity provider enter their credentials only once to access apps and desktops.

FAS servers connected with a single resource location

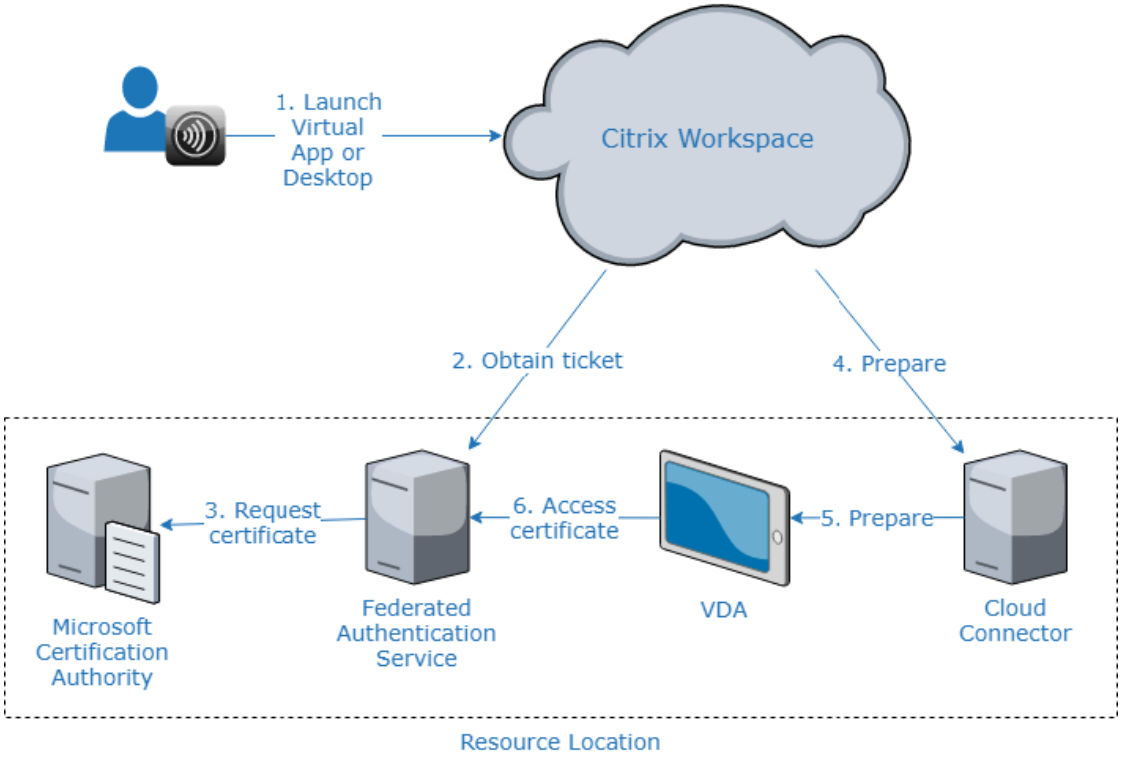
If your resource locations contain varied infrastructure (for example, different resource locations contain different AD forests), deploy FAS servers to the resource location where your VDAs are. SSO is active only in resource locations where one or more FAS servers are connected.

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 workspace subscribers 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 subscribers 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 subscriber, 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 subscribers 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 Workspace, 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 workspaces 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

The requirements in this section apply to all FAS servers that you plan to connect with Citrix Cloud.

Complete system requirements for the FAS server are described in the System Requirements section of the FAS product documentation.

FAS servers in your on-premises Citrix Virtual Apps and Desktops environment must have Federated Authentication Service 2003 (Version 10.1) or later installed.

If your existing FAS server is older than Version 10, you can download the latest FAS software from Citrix and upgrade the server in-place before creating this connection. When you create the connection, you select the resource location for your FAS server. SSO is active for subscribers only in the resource locations where FAS servers are present.

For more information about upgrading an existing FAS server, see Install and configure in the FAS product documentation. The same FAS server can be used for Workspace and on-premises deployments.

Citrix Workspace

You must have Citrix DaaS provisioned and enabled in Workspace. By default, the DaaS is enabled in Workspace Configuration after you subscribe to the service. However, the service requires that you deploy Citrix Cloud Connectors to allow Citrix Cloud to communicate with your on-premises environment.

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.

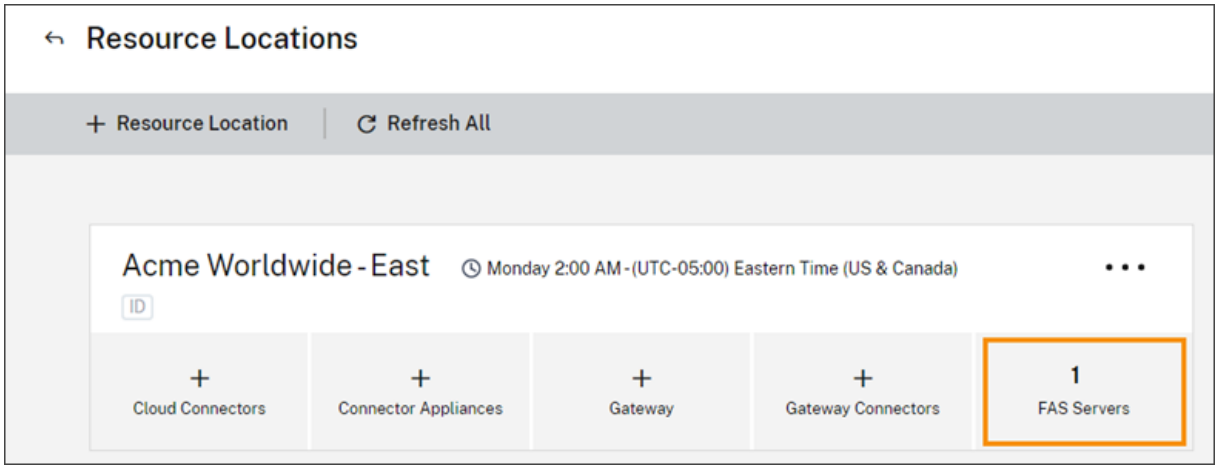
> **Tip:**
>
> You can also download the Federated Authentication Service installer from the Citrix Cloud console:

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.

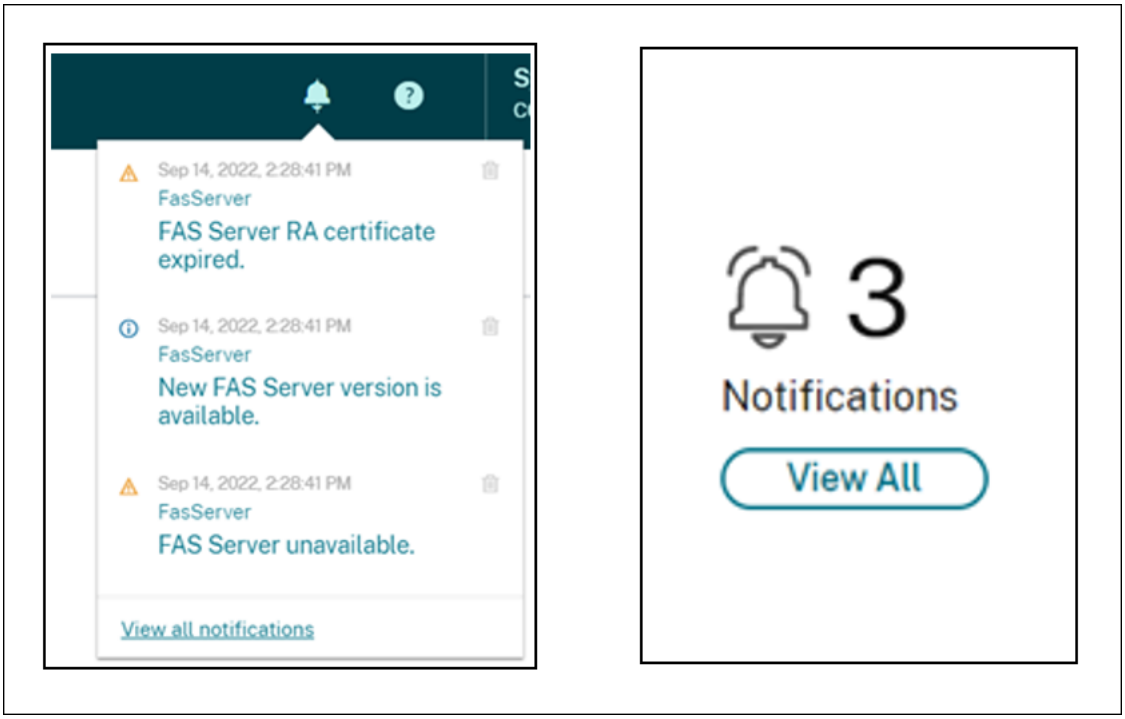
Support for Cloud notifications

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.

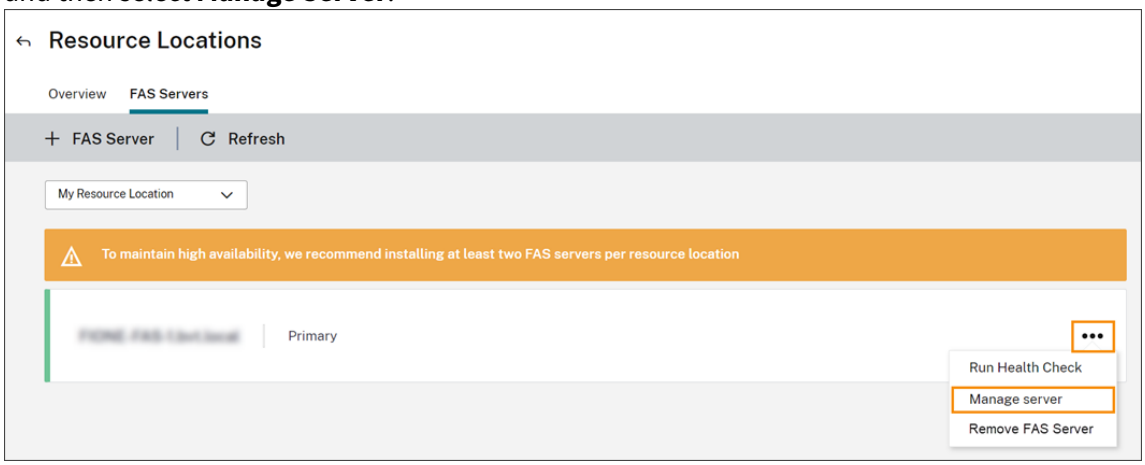


> **Note:**
>
> Once a notification is raised, it will be raised again periodically only if the issue is not resolved.

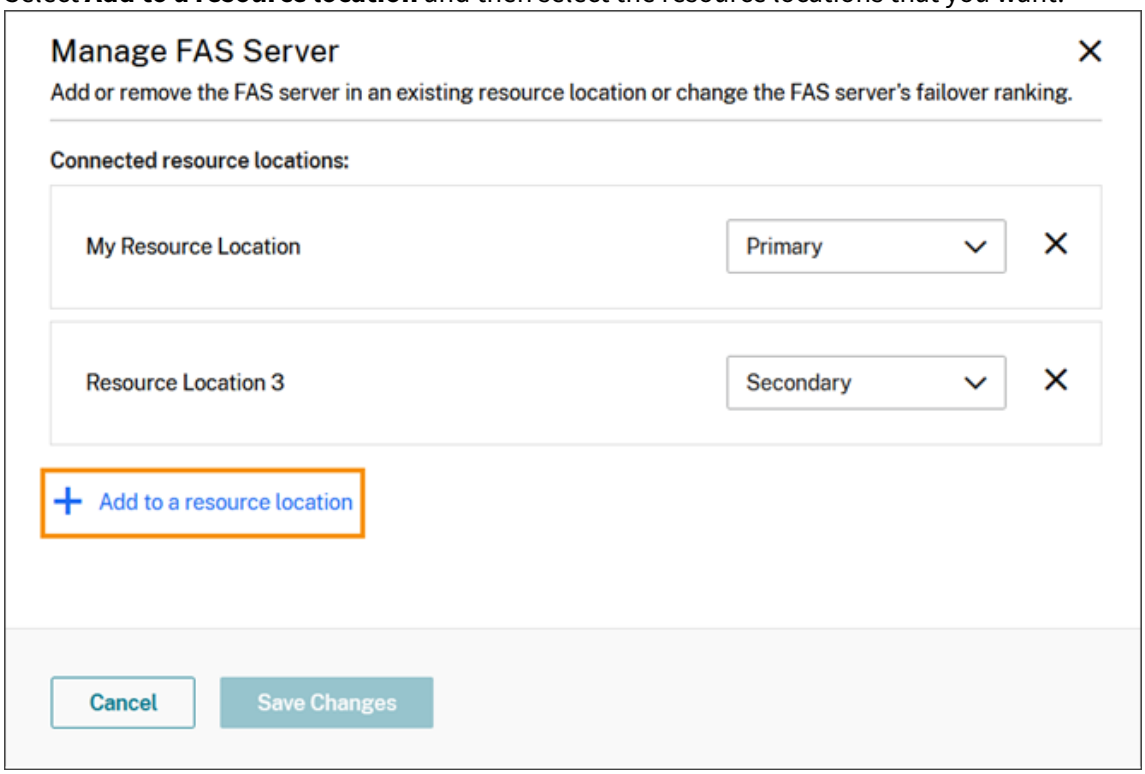
All notifications contain the FQDN of the impacted FAS server. The RA certificate expiry notification is displayed only for the FAS servers with version 10.10.0.14 and later.

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.

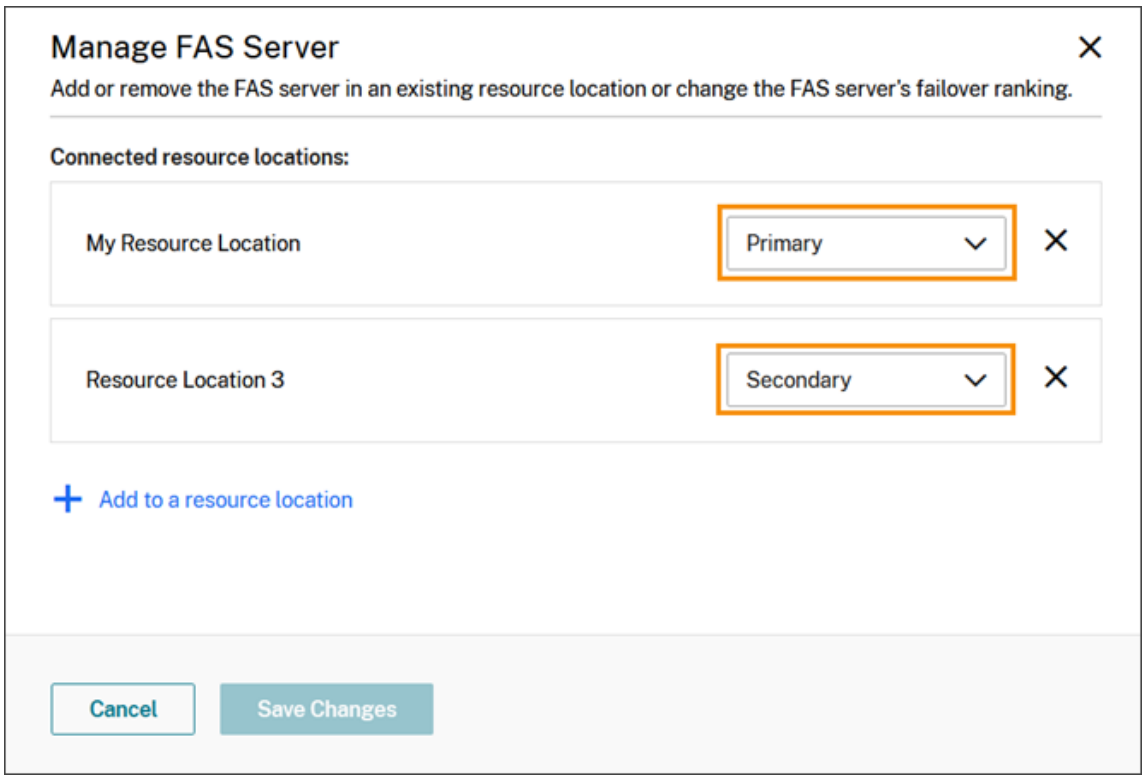


4. Select **Primary** or **Secondary** for the FAS server's failover priority in each selected resource location.
5. Select **Save Changes**.

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

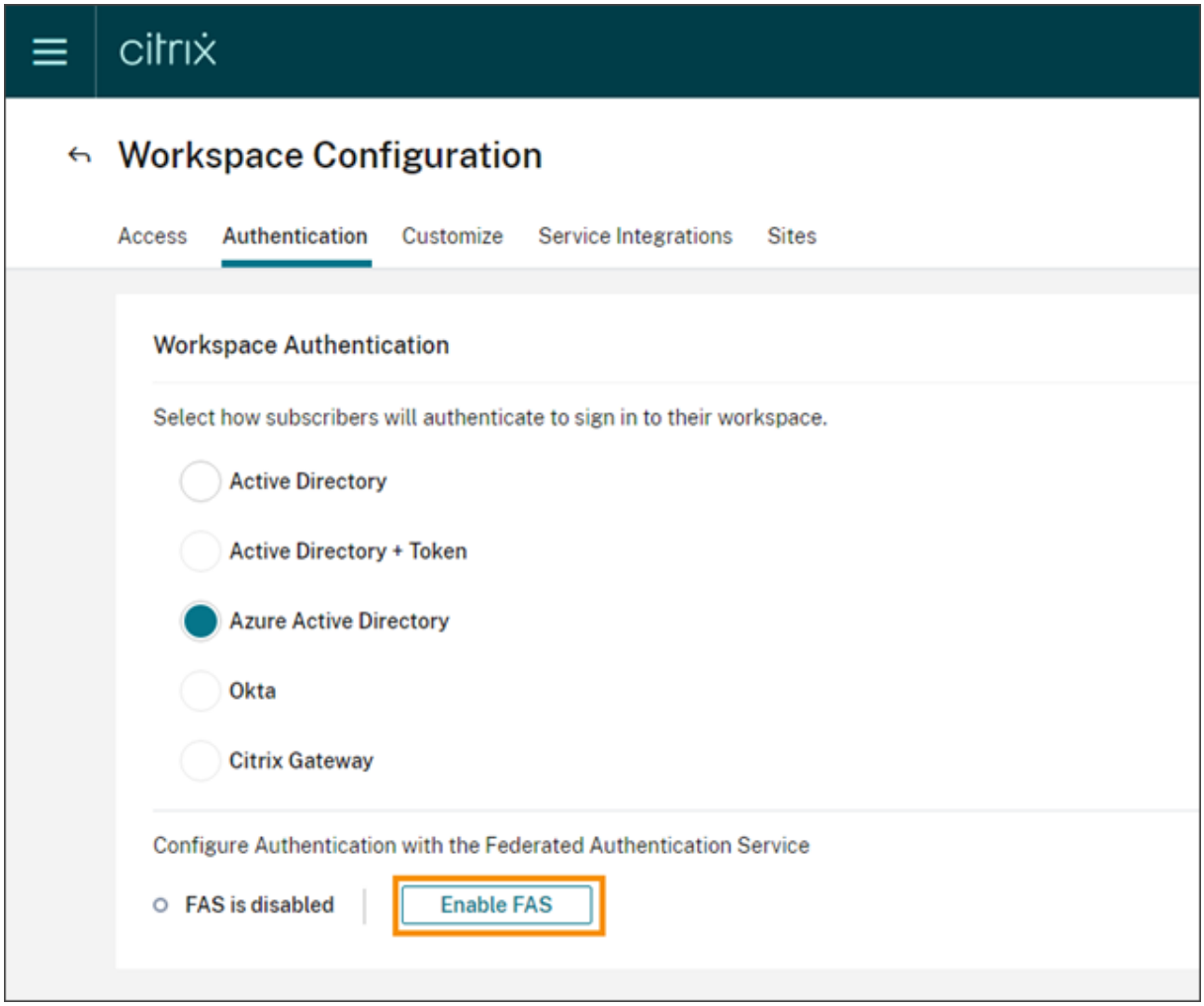
1. From the **Resource Locations** page, select the **FAS Servers** tile for the resource location you want to manage.
2. Select the **FAS Servers** tab.
3. Locate the FAS server you want to manage, click the ellipsis at the right side of the entry, and then select **Manage server**.
4. Locate the resource location with the priority you want to change and select the new priority from the drop-down list.



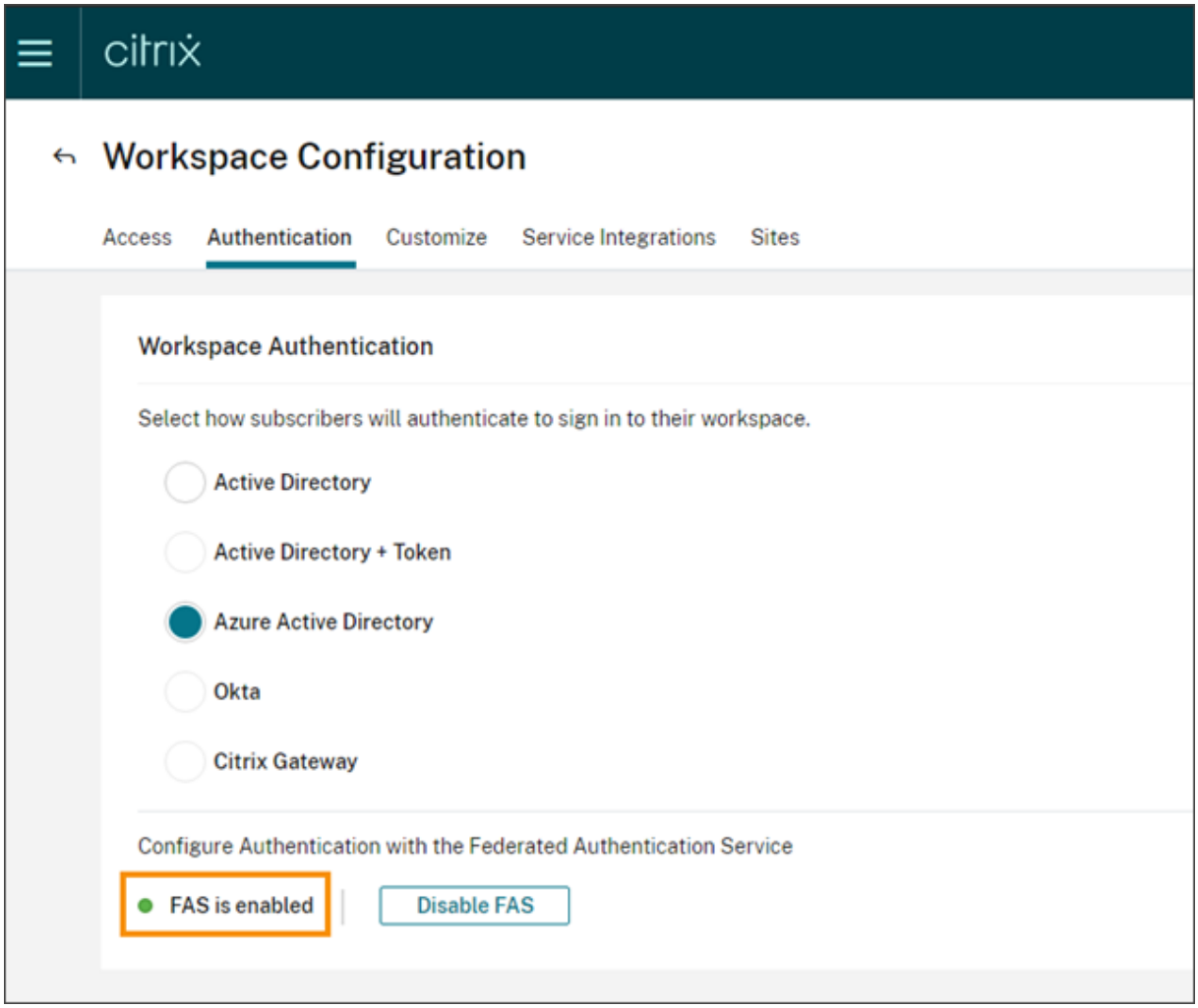
5. Select **Save Changes**.

Enable federated authentication for workspaces

1. From the Citrix Cloud menu, select **Workspace Configuration** and then select **Authentication**.
2. Click **Enable FAS**. This change might take up to five minutes to be applied to subscriber sessions.



Afterward, the Federated Authentication Service is active for all virtual app and desktop launches from Citrix Workspace.



When subscribers sign in to their workspace and launch a virtual app or desktop in the same resource location as the FAS server, the app or desktop starts without prompting for credentials.

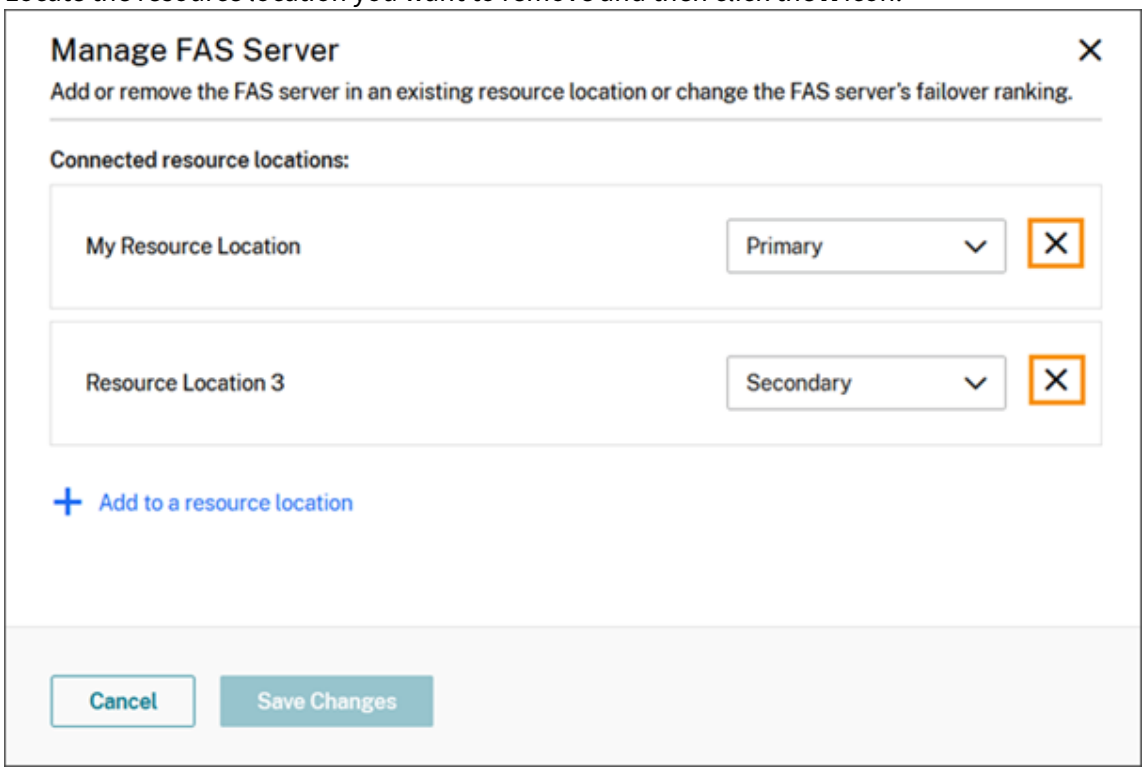
> **Note:**
>
> If all FAS servers in a resource location are down or in maintenance mode, application launches succeed, but single sign-on isn't active. Subscribers are prompted for their AD credentials to access each application or desktop.

Remove a FAS server

To remove a FAS server from a single resource location:

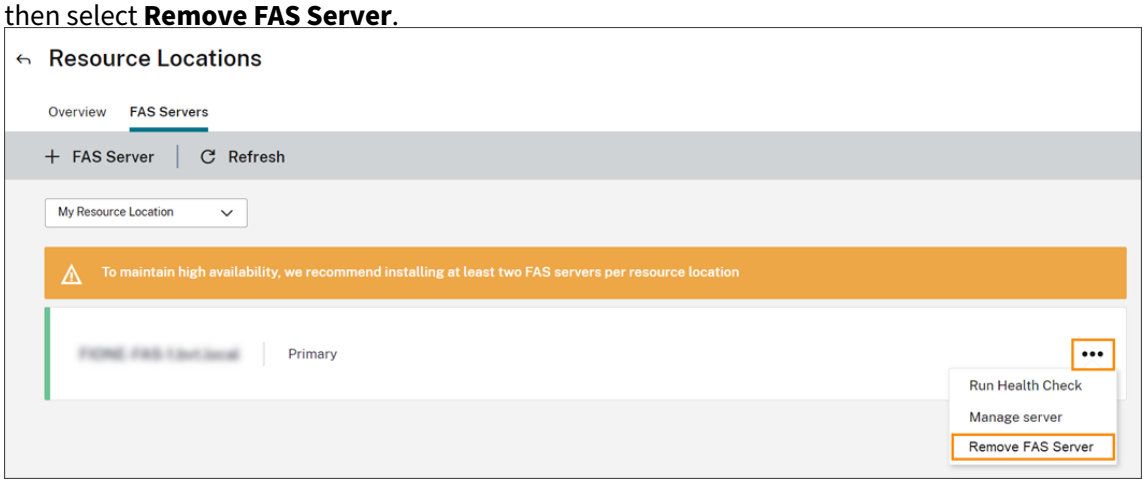
1. From the **Resource Locations** page, select the **FAS Servers** tile for the resource location you want to manage.
2. Select the **FAS Servers** tab.

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.

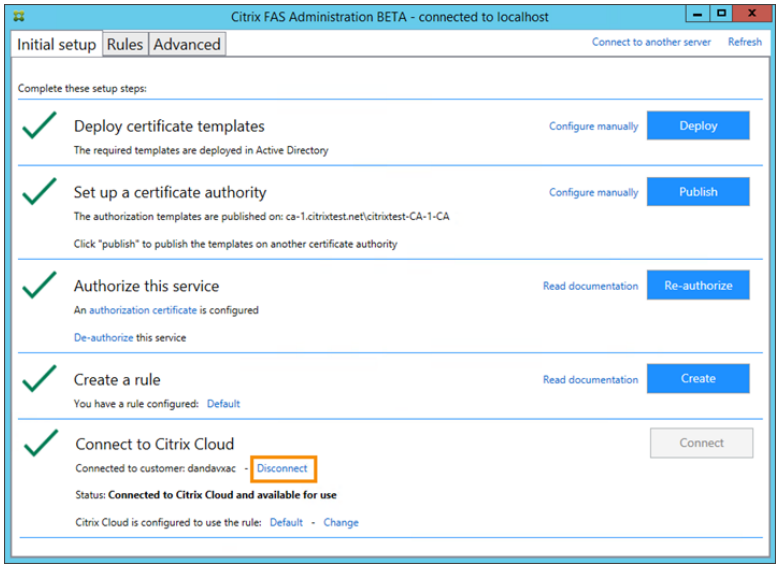


To remove a FAS server from all connected resource locations:

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**.

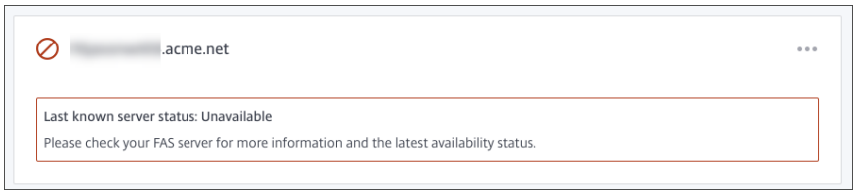


4. On the FAS administration console (on your on-premises FAS server), in **Connect to Citrix Cloud**, select **Disconnect**. Alternatively, you can uninstall FAS.

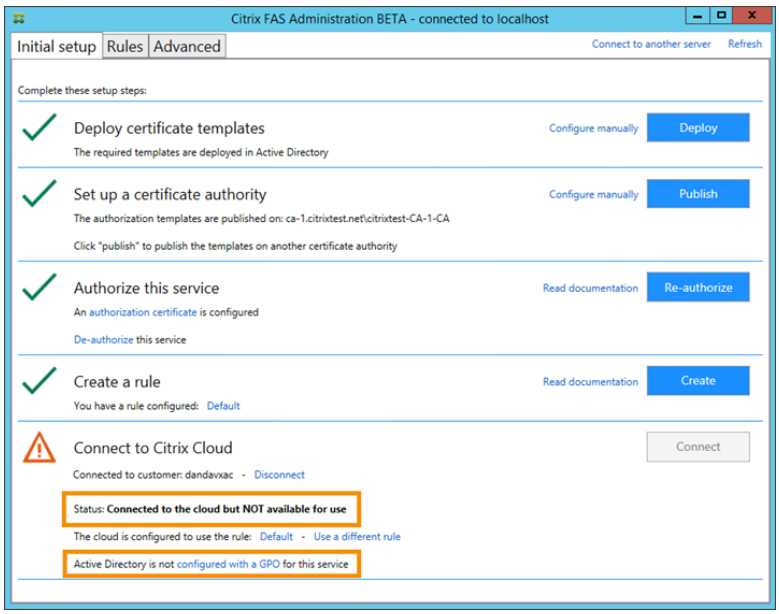


Troubleshooting

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