



Citrix Workspace

Contents

What's New	3
Get Started with Citrix Workspace	6
Citrix Workspace app and Citrix Receiver	9
Configure workspaces	14
Aggregate on-premises virtual apps and desktops in workspaces	50
Enable single sign-on for workspaces with Citrix Federated Authentication Service	59
Optimize connectivity to workspaces with Direct Workload Connection	70
Secure workspaces	81
Service continuity	89
Manage your workspace experience	110
Notifications in Workspace	116
Fall back to StoreFront	119
Optimize workflows	125
IT Self-service	128
HR Self-service	130
Sales Productivity	132
Employee Well-being	134

What's New

September 24, 2021

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](#).

September 2021

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](#).

New notification search feature: Workspace users are now able to search their activity feed and filter the results to find notifications from Microapps and integrations quickly. Users can also take action on notifications directly from the search results. For more information about this feature, see [Notifications in Workspace](#).

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 [Add a custom subscriber license agreement 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 for the duration of the reauthentication period as long as they are using their apps and desktops. For more information about this preview feature, see [Reauthentication period for 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. Additionally, 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 the Citrix RightSignature app, an electronic signature solution that comes bundled 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 [Electronic signature](#) and [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 Account Password to be Changed](#)

December 2020

Service continuity technical preview: 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](#).

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 Virtual Apps and Desktops services to deliver virtual apps and desktops. For more information, see [Citrix Cloud Government](#).

June 2020

Controlled feature rollout for Actions, Virtual Assistance, and Activity Feed: With the **Customize > Features** tab in Workspace Configuration, you can ensure your subscribers have the best experience with the newest Workspace features by rolling them out in a controlled manner. If you use AD, AAD, or Okta identity providers for workspace authentication, you can roll out Actions, Virtual Assistance, and Activity Feed to only the users and groups that you select or to all subscribers who have access to microapps. For more information, see [Actions, Virtual Assistance, and Activity Feed](#).

May 2020

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

December 2019

Microapps for Workspace: Microapps are now available to help you deliver relevant, actionable notifications from your applications directly into users' workspaces. With microapps, users can interact with key business systems without ever leaving their workspace, saving time and helping them focus on their day-to-day work. For more information, see [Microapps](#).

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 Virtual Apps and Desktops sessions. For more information about this

service and setup instructions, see [Optimize connectivity to workspaces with the Network Location Service](#).

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

Get Started with Citrix Workspace

May 26, 2021

Citrix Cloud provides a step-by-step guided walkthrough to help you get up and running quickly with Citrix Workspace. In the walkthrough, you'll learn about:

- Configuring a supported identity provider
- Adding administrators to your Citrix Cloud account
- Configuring the workspace URL for your organization
- Selecting the workspace authentication method for your end-users (also known as your workspace subscribers)
- Adding services to your new workspace

This article describes the technical information and resources you'll need at each step in the walkthrough.

Step 1: Build your workspace team

Engaging the right people and teams in your organization is essential for a successful workspace deployment. Use the following suggested roles to identify the people who can help you meet the technical requirements for delivering workspace resources to your end-users.

- Security and networking specialists: Ensures the requirements for Internet connectivity, Citrix Cloud Connector deployment, secure access to workspaces, and end-user authentication are met. You might also include these roles in testing your workspace to make sure your end-users can authenticate successfully and access their resources.
- Workspace and service administrators: Authorized to sign in to Citrix Cloud and administer Workspace Configuration settings and manage your purchased services. You might also include these roles in testing your workspace to make sure your end-users can access the resources they need.
- Communications manager: Educates your end-users about Citrix Workspace and how workspaces enhance the way they work.
- Training coordinator: Prepares the end-users in your organization for using workspaces as part of their daily work. This might include informal training sessions or self-service resources by email.

- **Support specialists:** Maintain the infrastructure you're using to provide workspace resources, support your end-users as needed, and troubleshoot any issues post-deployment. You might also include these roles in testing your workspace to make sure your end-users can access their resources.

Step 2: Configure an identity provider

Citrix Cloud supports a variety of identity providers to authenticate the end-users who access workspace resources. After you complete this step in the walkthrough, you can select your configured identity provider as the workspace authentication method in Step 4: Customize your workspace.

To learn more about the identity providers you can use with Citrix Workspace, see the following articles:

- [Identity providers](#): For a list of supported identity providers and links to the requirements and configuration instructions for each one.
- [Secure workspaces](#) (Citrix Workspace): For an overview of what your end-users experience with each supported workspace authentication method.
- [Citrix Cloud Connector](#): For requirements, deployment guidance, and instructions for connecting your environment with Citrix Cloud when you choose Active Directory, Citrix Gateway, or Okta as your identity provider.

Step 3: Add administrators

In this step, you invite the technical personnel you identified in Step 1: Build your workspace team to be administrators of your Citrix Cloud account. This step includes defining the access level for each administrator, such as access to Workspace Configuration and to manage the individual services you have purchased.

For more information about adding administrators to Citrix Cloud and access levels for services, refer to the following articles:

- [Add administrators to a Citrix Cloud account](#): Instructions for inviting administrators and setting access permissions.
- [Administrator access to Workspace Configuration](#): Instructions for enabling administrator access to Workspace Configuration settings.
- [Delegated Administration](#): Overview of the built-in roles and scopes for administering the Virtual Apps and Desktops service with instructions for assigning permissions and managing roles.

Step 4: Customize your workspace

In this step, take a moment to review the workspace URL that your end-users will use to access their workspace. If needed, you can change the first part of the workspace URL so it better reflects your company's name. For instructions, see [Workspace URL](#).

Also, select the workspace authentication method that your end-users will use when they sign in to their workspace. Remember, you configured the identity provider for this method in Step 2: Configure an identity provider. From the Citrix Cloud menu, select **Workspace Configuration > Authentication** and then select the workspace authentication you want to use.

Step 5: Integrate services

Now, you're ready to add your purchased services to Citrix Workspace. First, make sure your services are configured so they can provide the resources your end-users need. For more information and instructions, see the following articles:

- All services: [Service connectivity requirements](#)
- Content Collaboration:
 - [Deploy](#) provides guidance and instructions for enabling Content Collaboration for Citrix Workspace.
 - [Configure](#) provides instructions for adding administrators and users, configuring security, and managing reports.
 - [Citrix Files on Citrix Virtual Apps and Desktops](#) provides instructions for delivering Citrix Files through a virtual app or desktop that your end-users access in their workspace.
- Citrix Gateway:
 - [Support for Citrix Virtual Apps and Desktops](#) provides instructions for enabling secure access to Virtual Apps and Desktops resources.
 - [Support for Software as a Service apps](#) provides requirements and instructions for enabling secure access to SaaS apps that you want to make available through Citrix Workspace.
 - [Support for Enterprise web apps](#) includes requirements and instructions for enabling secure access to enterprise web apps that you want to make available through Citrix Workspace.
- Microapps:
 - [Getting Started](#) provides an overview of the required tasks for setting up Microapps with Citrix Workspace and creating integrations.
- Endpoint Management: [Onboarding and resource setup](#)
- Virtual Apps and Desktops: [Install and configure](#)

After you've configured your purchased services, follow the steps in [Enable and disable services](#) to ensure end-users can see and access these resources in their workspace.

Test your workspace

Sign in to your workspace using the workspace URL, verify you can authenticate successfully, and access the resources that your end-users will need to perform their daily work. Depending on the services you purchased, the technical personnel you identified in Step 1: Build your workspace team might include the following tests:

- Signing in to your workspace as an administrator and as an actual end-user, using a web browser and using [Workspace app](#) on a computer or mobile device
- Launching and using apps and desktops, including any enterprise web apps and SaaS apps
- Accessing endpoint resources through an enrolled mobile device
- Accessing folders and files from the Citrix Files pane of your workspace
- Verifying the Actions pane of your workspace displays the actions that your microapps integrations make available to end-users
- Completing an action from the Actions pane of your workspace to verify your microapps are working with your organization's data sources

Roll out workspaces to end-users

Congratulations, your workspace is ready to go live! Help your end-users learn how Citrix Workspace can help them do their work more effectively with these resources:

- [Citrix Workspace end-user adoption resources](#)
- [Content Collaboration user adoption kit](#)
- [Virtual Apps and Desktops end-user adoption resources](#)
- [Endpoint Management end-user adoption resources](#)

The communications and training specialists you identified in Step 1: Build your workspace team can use these resources to build awareness, communicate the value of workspaces, enlist champions across your organization, and provide ready-to-use guides and instructions for using Workspace app. They can also partner with your technical specialists to address end-user feedback and identify lessons learned throughout the roll-out process.

Citrix Workspace app and Citrix Receiver

March 23, 2021

Citrix Workspace app replaces and extends the full capabilities of Citrix Receiver. Citrix recommends using the latest version of Citrix Workspace app to access workspaces. You can also access workspaces using Internet Explorer 11, or the latest version of Edge, Chrome, Firefox, or Safari.

For more information about supported features in Workspace app by platform, refer to the [Workspace app feature matrix](#).

Important lifecycle milestone for Citrix Receiver

Citrix Receiver has reached End of Life and is no longer supported. If you continue to use Citrix Receiver, technical support is limited to the options described in [Lifecycle Milestones Definitions](#).

For more information about End of Life milestones for Citrix Receiver by platform, refer to [Lifecycle Milestones for Citrix Workspace app and Citrix Receiver](#).

Information in this article about Citrix Receiver is provided as a convenience to help you transition your subscribers to using Workspace app.

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 or 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 Workspace app support for specific features, refer to the [Workspace app](#)

[feature matrix](#).

For an overview of TLS and SHA2 support with Citrix Receivers, see [CTX23226](#).

Transitioning from Citrix Receiver to Citrix Workspace app

This section guides existing customers who are working with Citrix Receiver through the change to Citrix Workspace app.

The latest Citrix Workspace experience is available with the following services in Citrix Cloud:

- Virtual Apps Essentials
- Virtual Desktops Essentials
- Virtual Apps and Desktops service (includes Site aggregation from Virtual Apps and Desktops on-premises resources)
- Citrix Gateway service (delivering secure web and SaaS apps)
- Content Collaboration (formerly ShareFile)
- Secure Browser service

New customers. If you're new to the workspace experience, you'll get the latest version of the user interface as soon as it is available. You can access the workspace experience from your browser or from a local Citrix Workspace app.

Existing customers. If you've been using an earlier version of Citrix Workspace, the updated user interface can take around five minutes to display in local Citrix Workspace apps. You may temporarily see an older version of the user interface. Alternatively, you can click the **Refresh** button in your web browser to update the user interface as needed. If you've been using Citrix Receiver, guide users to upgrade to Citrix Workspace app so they can use all the features of Citrix Cloud services.

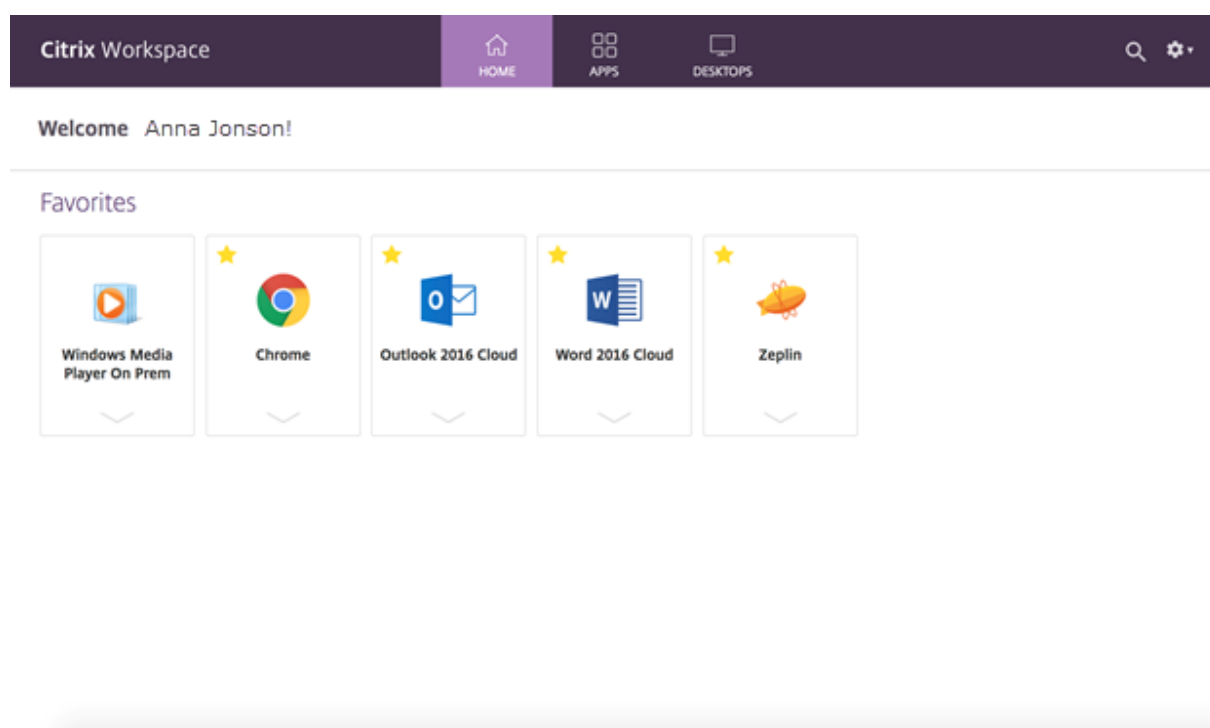
The following scenarios illustrate what users are likely to see if they are still using Citrix Receiver rather than Citrix Workspace app (recommended).

Citrix Receiver

Important:

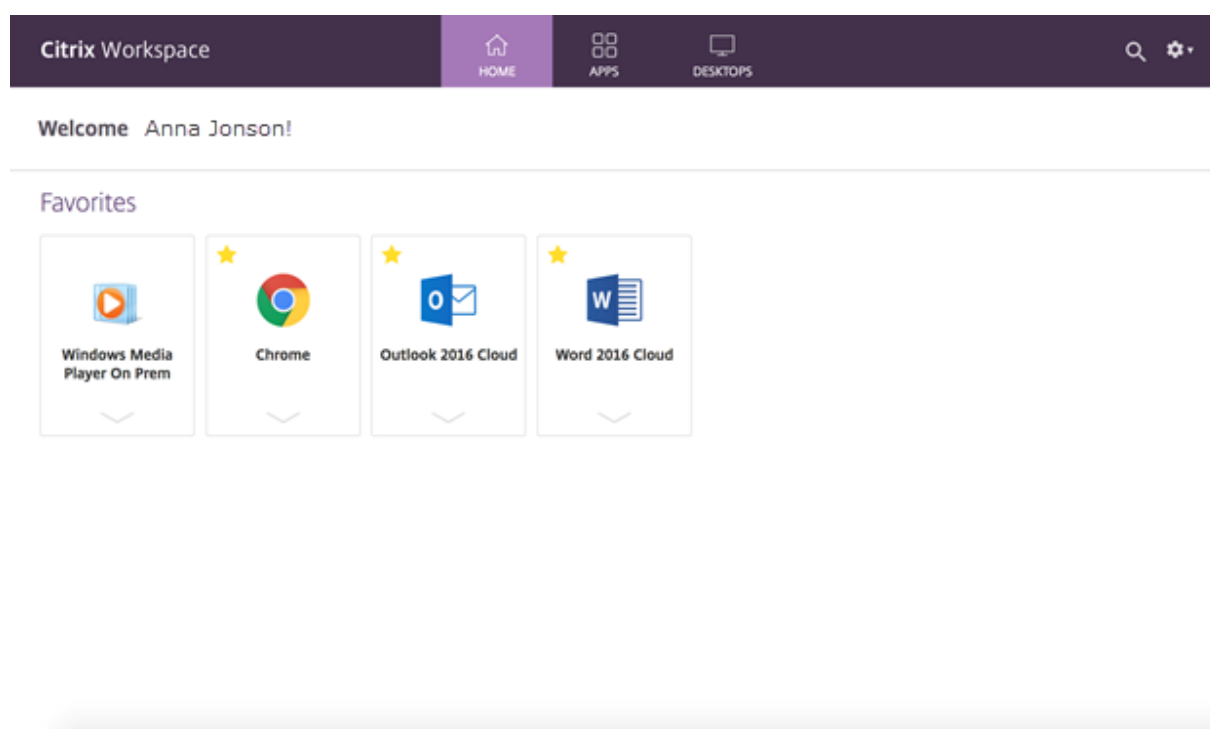
Citrix Receiver has reached End of Life. For more information, refer to Important lifecycle milestone for Citrix Receiver in this article.

Users that are still accessing Workspace with Citrix Receiver see the “purple” user interface shown below. They see Virtual Apps and Desktops apps as well as web and SaaS apps from the Citrix Gateway service. Files are not supported in Citrix Receiver and users cannot access them this way.



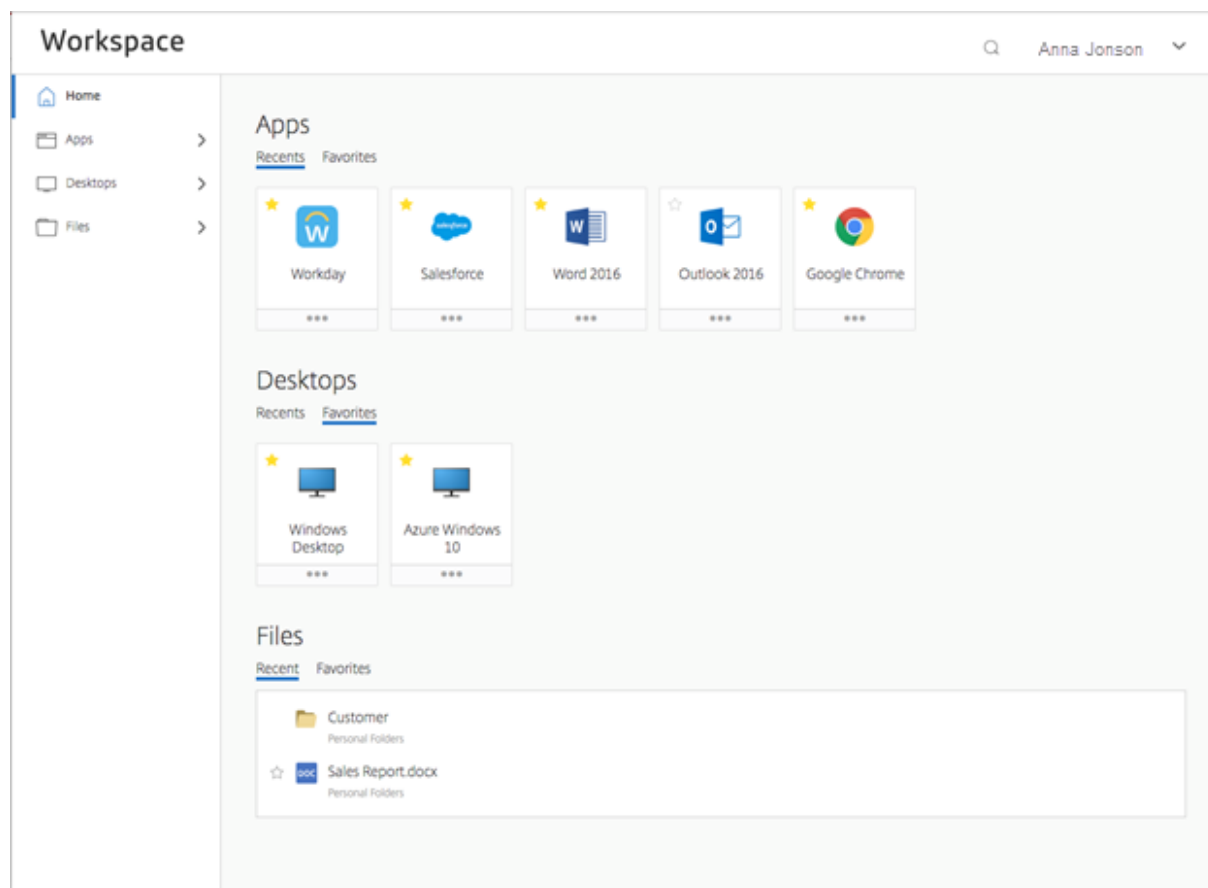
The access control feature is not supported in Citrix Receiver. Thus, with the same services and **access control** enabled, users still see the purple user interface, but without web and SaaS apps.

Access control is a feature that delivers access for end users to SaaS, web, and virtual apps with a single sign-on (SSO) experience.



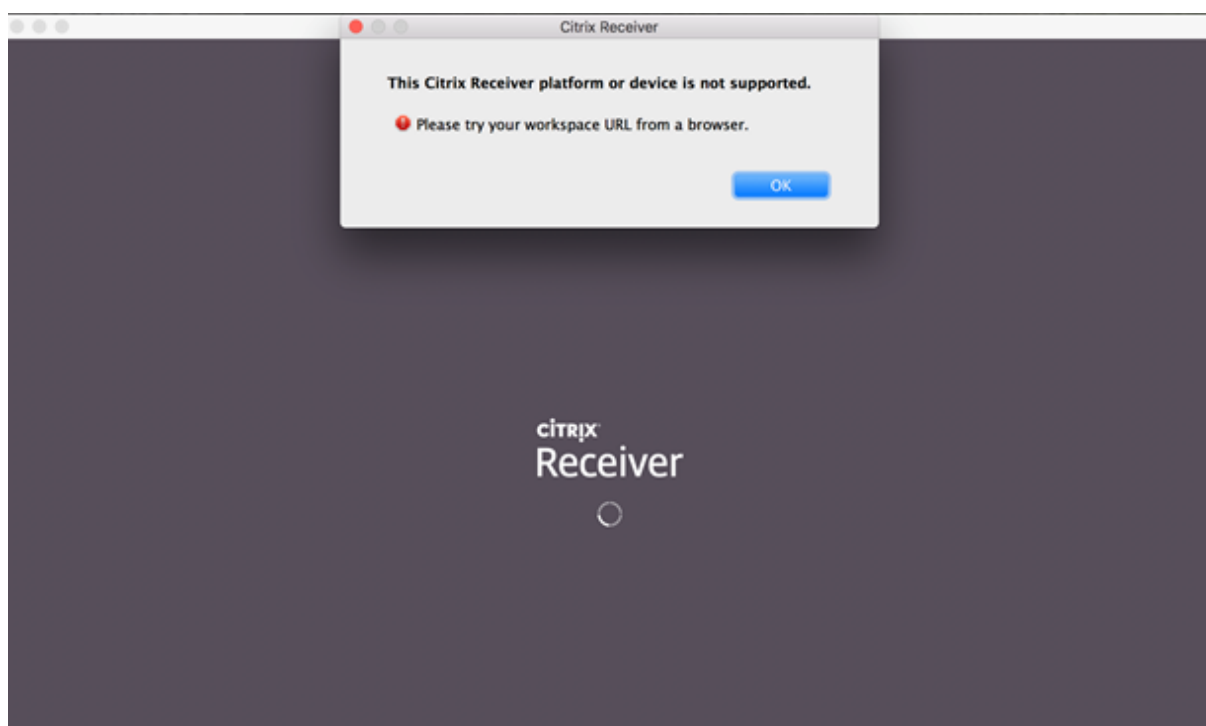
Citrix Workspace app or browser

Users that upgrade to Citrix Workspace app or use a web browser to access Workspace see the new user interface. They can then use all the new functionality, including access to Files.



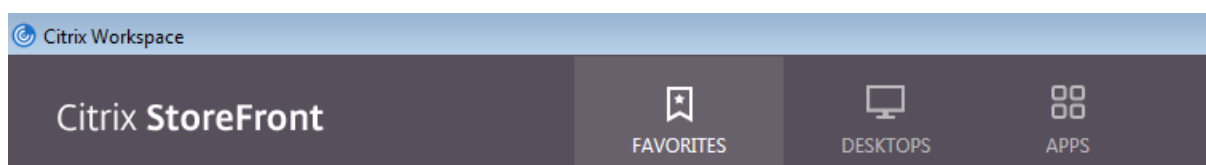
Azure Active Directory (AAD)

This scenario is for when AAD is enabled as the Workspace authentication method. If users try to access Workspace with Citrix Receiver, they'll see a message that the device isn't supported. Once they upgrade to Citrix Workspace app, they can access their workspace.



StoreFront (on-premises deployment)

This scenario is for a StoreFront on-premises environment. If users choose to upgrade from Citrix Receiver to Citrix Workspace app, the only change will be the icon to open Citrix Workspace app.



Government users

[Citrix Cloud Government](#) users will continue to see their “purple” user interface when using the Workspace app or when accessing from a web browser.

Configure workspaces

September 28, 2021

This article describes how to configure workspaces for subscribers, who might be using one or more services available from Citrix Cloud.

Note:

Looking for workspace authentication articles?

Secure workspaces is the new home for information about supported methods for subscriber authentication to workspaces. See the following sections:

- [Active Directory](#)
- [Azure Active Directory](#)
- [Active Directory plus token](#)
- [Citrix Gateway](#)
- [Okta](#)

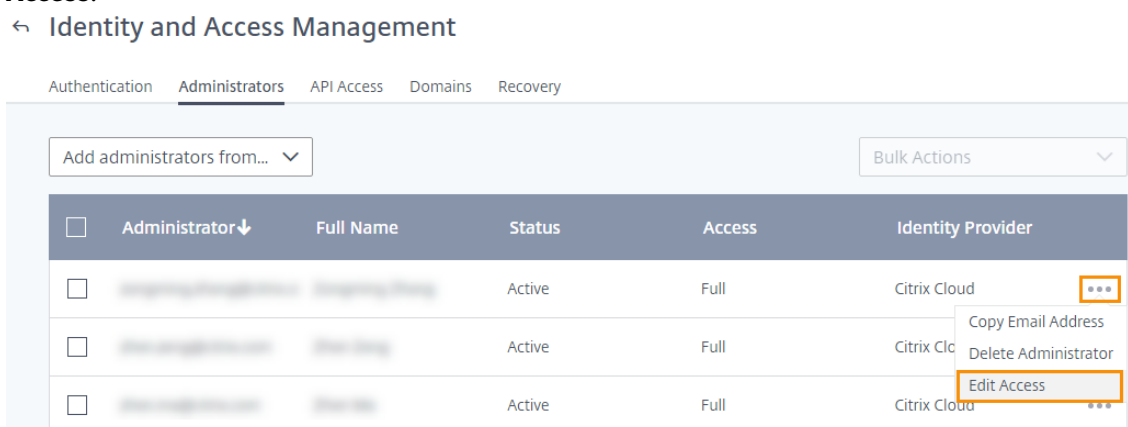
For information about single sign-on for workspace subscribers, see [Enable single sign-on for workspaces with Citrix Federated Authentication Service](#).

Administrator access to Workspace Configuration

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 you select.

To enable access to Workspace Configuration:

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

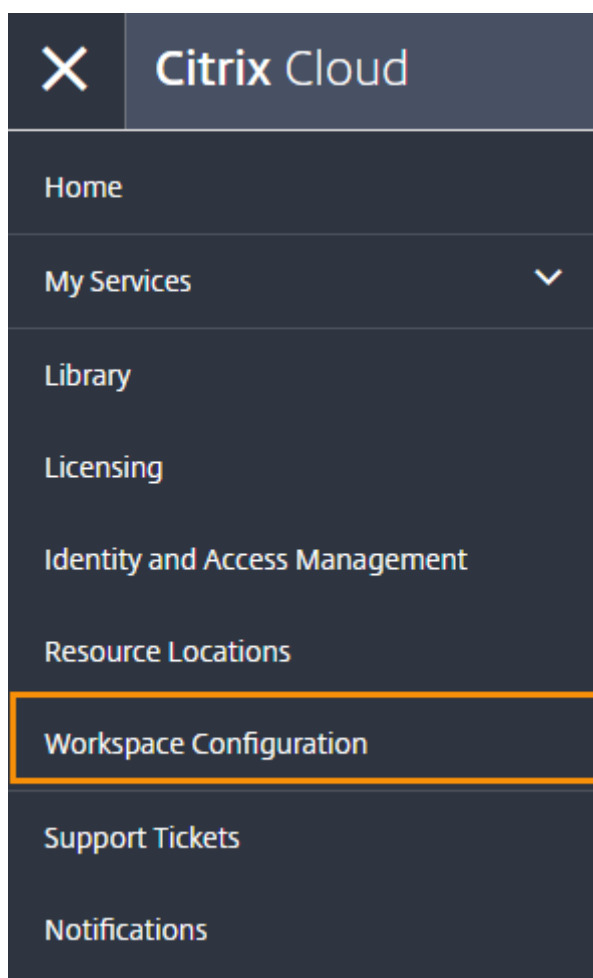


3. Verify that **Custom Access** is enabled.
4. To enable only Workspace Configuration access, under **General Management**, select **Workspace Configuration**. Selecting **General Management** enables all permissions in the group.

- ☐ Full access
Full access allows administrators management control of Citrix Cloud and its services, as well as adding or removing other administrators.
- ☒ Custom access
[i](#) Switching to custom access will remove management access to certain services.
Custom access allows you to determine exactly which part of Citrix Cloud your administrators can manage.
[Select all](#) | [Deselect All](#)

- ☐ General Management
-
- ☐ Domains
- ☐ Library
- ☐ Notifications
- ☐ Resource Location
- ☒ Workspace Configuration

After enabling access, administrators sign in to Citrix Cloud and select **Workspace Configuration** from the **Citrix Cloud** menu.



Connectivity requirements

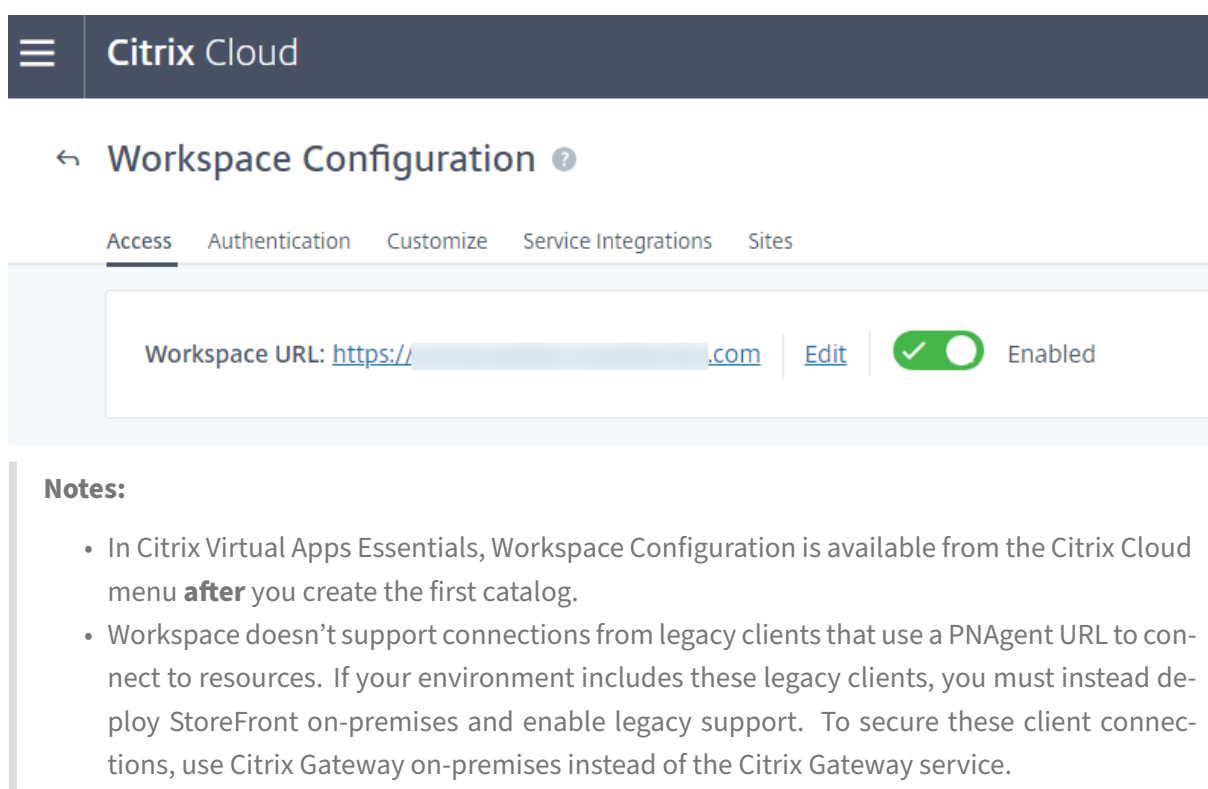
The following addresses must be contactable to operate and consume Citrix Workspace:

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

For a complete list of required contactable addresses for Citrix Cloud services, see [Service connectivity requirements](#).


Workspace URL

In **Citrix Cloud > Workspace Configuration > Access**, the Workspace URL is ready to use.



Workspace Configuration ?

Access Authentication Customize Service Integrations Sites

Workspace URL: <https://.com> [Edit](#)  Enabled

Notes:

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

Customize the workspace URL

The first part of the workspace URL is customizable. You can change the URL from, for example, <https://example.cloud.com> to <https://newexample.cloud.com>.

Important:

The first part of the workspace URL represents the organization using the Citrix Cloud account, and must comply with the [Citrix End User Services Agreement](#). Misuse of third party intellectual property rights, including trademarks, might result in revocation and reassignment of the workspace URL or suspension of the Citrix Cloud account.

From the **Citrix Cloud** menu, go to **Workspace Configuration > Access**, and select the **Edit** link next to the workspace URL.

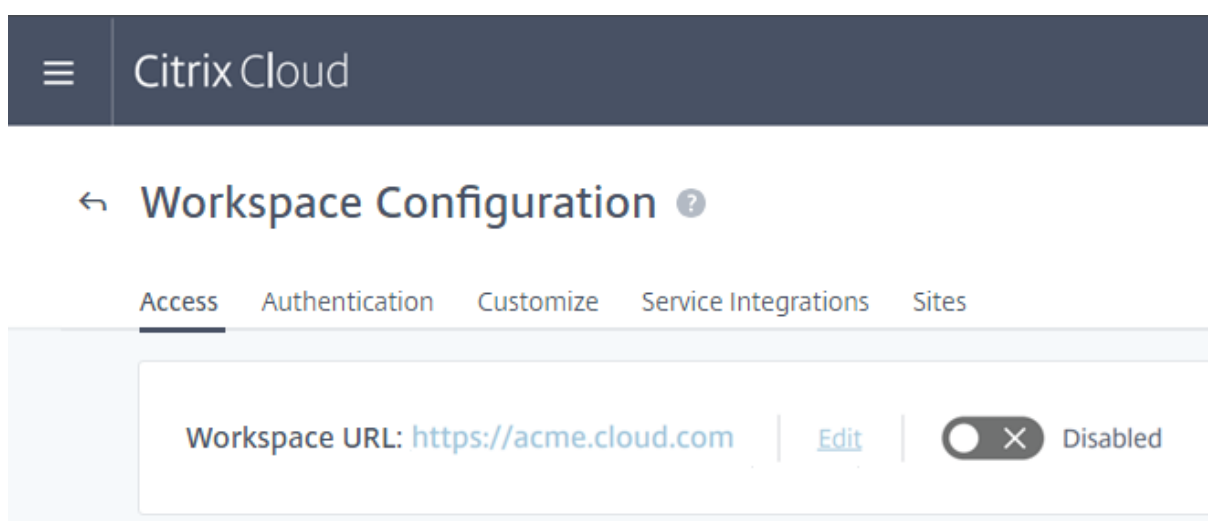
Guidance for new URLs:

- The customizable part of the URL (“newexample”) 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.
- The customizable part of the URL must consist of only letters and numbers.
- The customizable part of the URL can't include Unicode characters.
- When you rename a URL, the old URL is immediately removed and no longer available.

- If you change the workspace URL, your subscribers can't access their workspaces until the new URL is active, which takes about 10 minutes. Tell subscribers what the new URL is and manually update all local Citrix Receiver apps to use the new URL.
- You can change the workspace URL only when it's enabled. If the URL is disabled, you must re-enable it first. Re-enabling the workspace URL can take up to 10 minutes to take effect.

Disable the workspace URL

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



Disabling or re-enabling the workspace URL can take up to 10 minutes to take effect. After the workspace URL is disabled, Citrix Cloud parks the domain so it can't be accessed. Anyone visiting the URL receives a 404 message in their browser.

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.

External connectivity

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

Citrix supports these connectivity options:


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

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

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

Workspace Configuration

Access Authentication Customize Service Integrations Sites

Workspace URL: <https://.com> [Edit](#)  Enabled

External Connectivity

Set up connectivity for each resource location that will be used for subscriber access to your workspace.

[Learn more about resource locations.](#)

Virtual Apps and Desktops:

AWS Gateway Service	...
Azure Gateway Service	...
My Resource Location Gateway Service	...

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.

Enable and disable services

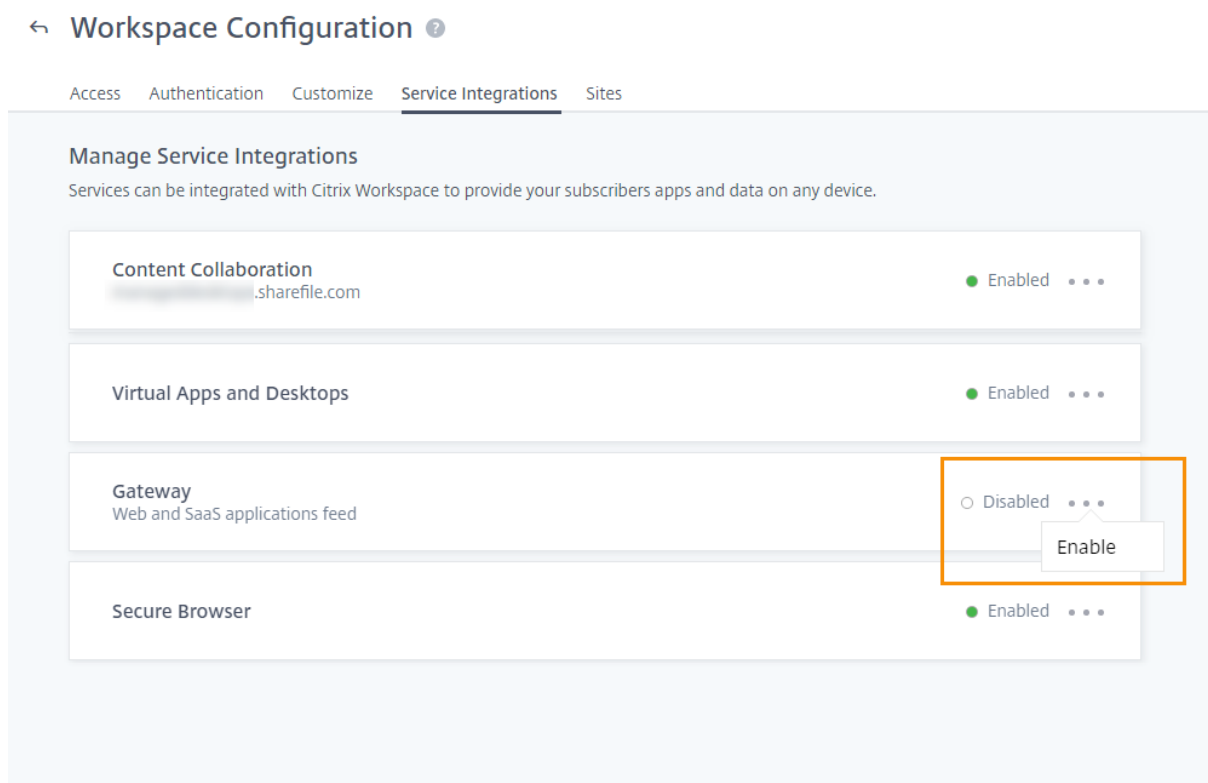
You can enable or disable the availability of individual service resources from the **Service Integrations** tab. Subscribing to the Virtual Apps and Desktops service and the Secure Browser service enables them by default. All other new services that your organization subscribes to are disabled by default.

Note:

Citrix App Essentials service, Citrix Desktop Essentials service, and Citrix Virtual Apps and Desktops service display as "Citrix Virtual Apps and Desktops service" in the Service Integrations tab.

To enable workspace integration for a service

1. Go to **Workspace Configuration > Service Integrations**.
2. Select the ellipsis button next to the service and then select **Enable**.
3. To disable integration, select the ellipsis button next to the service and then select **Disable**.



To disable workspace integration for a service

Important:

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.

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



Subscribers will no longer have access to data and applications from this service in Citrix Workspace

Are you sure you want to disable workspace integration for Virtual Apps and Desktops?

Cancel

Confirm

Customize the appearance of workspaces

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	350 x 120 pixels	2 MB	JPEG, JPG, or PNG
After 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.

Workspace Configuration

Access

Authentication

Customize

Service Integrations

Sites

Service Continuity

Appearance

Features

Preferences

Customize how subscribers will see their workspace.

Cancel


Update

Default Appearance

Sign-in Appearance

Logo


This logo will appear on the sign-in page.



After Sign-in Appearance

Logo

This logo will appear after sign-in.




Colors


These colors appear in sign-in screens and within the workspace experience.


Banner color:

Accent color:

Banner text and icon color:







Preview

This is how your workspace will look:

Home

Apps


Desktops

Files

Apps


Recents

Favorites




App Title

...




App Title

...




App Title

...




App Title

...



App Title

...



App Title


...

Reset to Default

Appearance themes

Apply an appearance theme to override the default for a specific set of users. [Learn more](#)

+ Add 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.



The image shows the Citrix Workspace sign-in page. At the top center is the Citrix logo, a stylized 'C' made of three concentric arcs. Below the logo is the text 'Citrix Workspace' in a large, dark blue font. Underneath is a 'Username' label followed by a text input field containing the placeholder text 'domain\user or user@domain.com'. Below that is a 'Password' label followed by a text input field containing the placeholder text 'Enter password'. At the bottom is a large, rounded teal button with the text 'Sign In' in white.

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 more information on how to customize an Azure AD sign-in page, see the [Microsoft documentation](#). For more information on how to customize the Okta-hosted sign-in page, see the [Okta Developer documentation](#).

You can also customize the on-premises Citrix Gateway sign-in page. You configure this 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 (Technical Preview)

Important:

- The ability to create, customize, and prioritize multiple themes is in **Private Technical Preview**. Citrix recommends you use technical preview features only in test environments. To sign up for this technical preview, visit <https://podio.com/webforms/25197371/1860213>.
- This is 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.

Workspace Configuration

Access Authentication **Customize** Service Integrations Sites Service Continuity

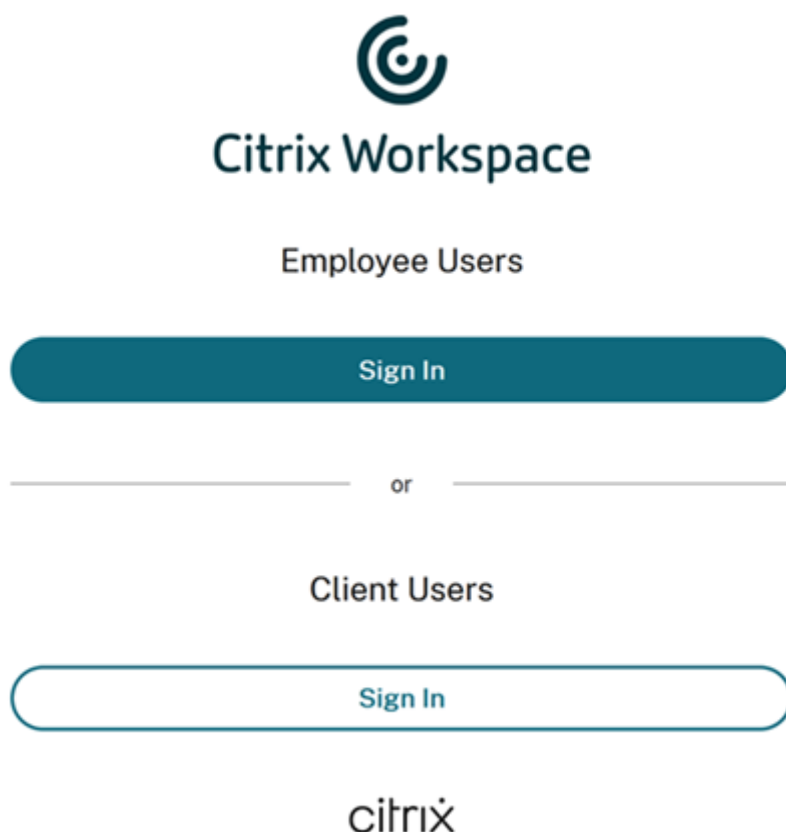
Appearance Features Preferences

Customize how subscribers will see their workspace. [Edit priority](#) [Add theme](#)

Theme Name	Description	Logo	Actions
Default appearance	Applied by default to all users not assigned to another theme.	ACME corporation	Edit
My First Policy	1 user group Priority 1	citrix	... Edit
My Second Policy	1 user group Priority 2	Citrix Workspace	... Edit

Note:

If you have Citrix Content Collaboration configured, only employee users see custom themes. Users who sign in to Citrix Workspace as a client user to access shared files through Citrix Content Collaboration only see the default theme.



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).

Add an appearance theme ✕

Apply an appearance theme to override the default for a specific set of users. [Learn more](#)

After Sign-in Appearance • Theme Details

Logo
This logo will appear after sign-in.



Colors
These colors appear in sign-in screens and within the workspace experience.

Banner color: 

Accent color: 

Banner text and icon color: 

[Save](#) [Preview](#) [Cancel](#) 

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

Add an appearance theme ✕

Apply an appearance theme to override the default for a specific set of users. [Learn more](#)


After Sign-in Appearance • **Theme Details**


Name your theme ⓘ

Assign users and groups ⓘ

Select an identity provider

Search for a group to add



[Save](#) [Preview](#) [Cancel](#) 

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.

Add an appearance theme ✕

Apply an appearance theme to override the default for a specific set of users. [Learn more](#)

After Sign-in Appearance

Theme Details

Name your theme ●

My First Policy

Assign users and groups: ●

Select an identity provider

Active Directory

Select a domain

domain.com

Search for a group to add

group



User groups (1):

Group



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

Note:

The **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.

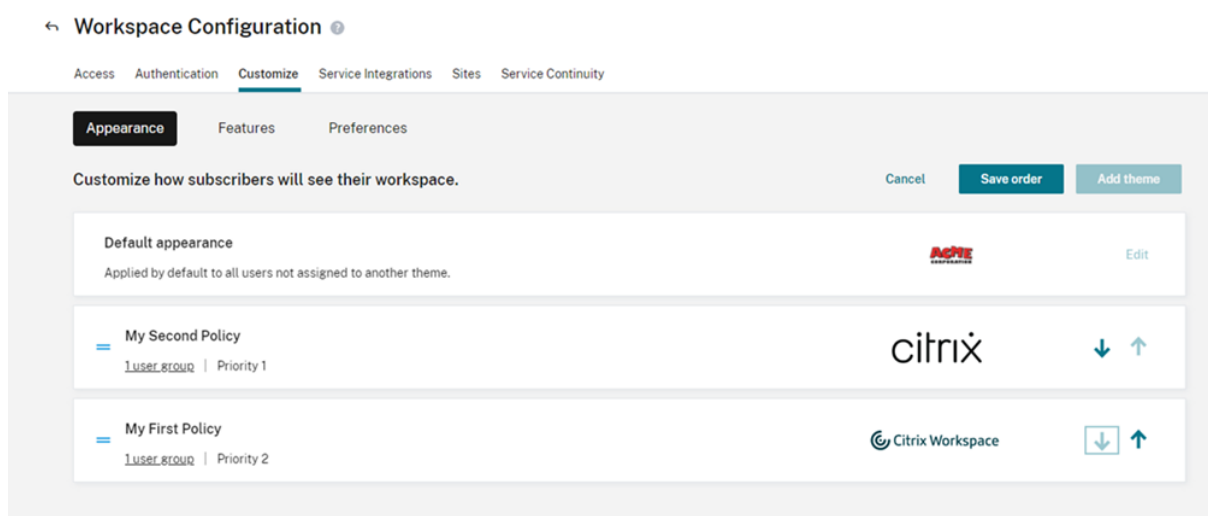
Prioritize custom themes

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 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**.

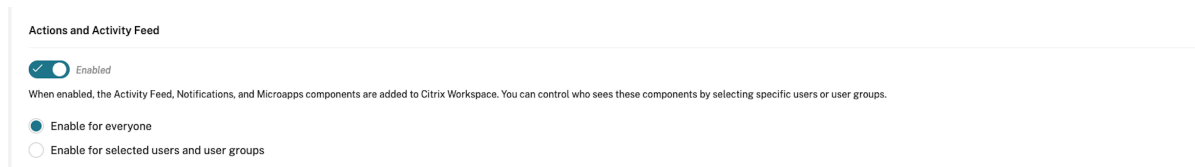


Customize rollout of new features

In **Workspace Configuration > Customize > Features**, you can roll out the newest Citrix Workspace features gradually for the best workspace experience for your subscribers. You can control this rollout by selecting the intended users and groups of the feature. When you're ready for all subscribers to use the feature, you can enable it easily for everyone.

Actions and Activity Feed

Enable features that help subscribers save time and accomplish work tasks more effectively, without leaving their workspace in **Workspace Configuration > Customize > Features**.



Using microapps, you can build integrations from your organization's application data sources to pull actions from those applications into your subscribers' workspace. Using microapps, subscribers can act on work items inside their workspace. For more information, see [Getting Started](#) in the Microapps documentation.

Requirements for configuration

Using the **Actions and Activity Feed** setting requires the following items:

- The [Microapps](#) service is enabled in **Workspace Configuration > Service Integrations**.

- You've subscribed the appropriate users and groups to the microapps that generate actions in the activity feed. For instructions, see [Managing subscribers](#).
- To enable the feature for specific users and groups, you must use one of the following authentication methods:
 - Active Directory
 - Active Directory + Token
 - Azure Active Directory
 - Okta

You can only enable or disable this feature for all microapps subscribers if:

- You're using Citrix Gateway as an identity provider.
- You're using the Citrix Federated Authentication Service with Citrix Cloud.

Configure the setting

After enabling the setting, choose whether to enable actions and activity feeds for all workspace subscribers with a microapps subscription or only for specific users and groups.

Actions and Activity Feed

☒ Enabled

When enabled, the Activity Feed, Notifications, and Microapps components are added to Citrix Workspace. You can control who sees these components by selecting specific users or user groups.

☒ Enable for everyone

☐ Enable for selected users and user groups

If you select **Enable for selected users and groups**, select the domain and search for the users and groups that should see the activity feed in their workspace. When you're finished adding users and groups, select **Save**.

Give your users a more robust experience by enabling feature-rich options to optimize their work.

SavePreview

Actions and Activity Feed

✓

Enabled

When enabled, the Activity Feed, Notifications, and Microapps components are added to Citrix Workspace. You can control who sees these components by selecting specific users or user groups.

Enable for everyone

Enable for selected users and user groups

i

Microapps are available only for users and groups that are entitled to them. To manage entitlements, visit the Microapps service via the [launchpad](#).

Assign Users and Groups

Step 1: Choose a directory

Step 2: Select a user or group

acmewww.com

▼

Search users or user groups

Q

Type

Display Name

Account Name ↑

Nothing to see here...

Use the search box to find users or groups to assign to this feature.

To remove users or groups, under **Assign Users and Groups**, select the trash can icon for the user or group and then select **Remove**.

GROUP	Building Security	company/groupname	<div><div></div><div></div></div>
USER	Bailey Simon	company/baileys	<div><div>Remove</div><div>X</div></div>

© 1999–2021 Citrix Systems, Inc. All rights reserved.

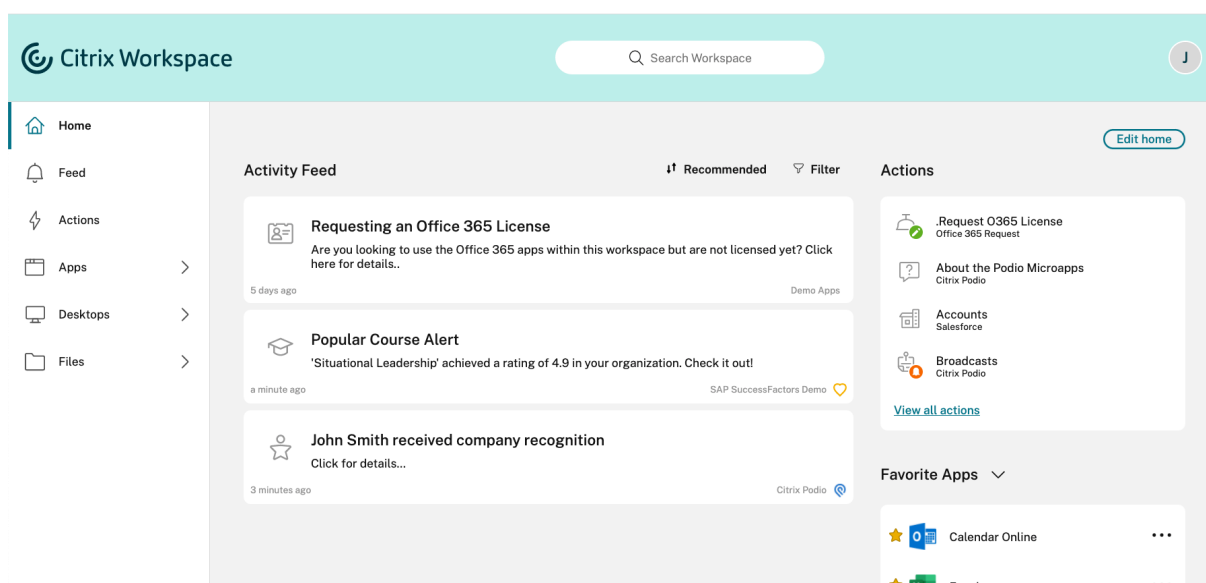
31

Preview the workspace

To see what your subscribers' workspace looks like with and without the activity feed, select **Workspace Configuration > Customize > Features > Preview**.

Subscriber experience with Actions and Activity Feed

When enabled, subscribers see personalized alerts and notifications in their **Activity Feed**, in the center of their workspace.



Subscribers don't have to switch to another application to complete actions. A subscriber can act on an item, such as approving a request, directly in the activity feed.

Actions on the right side of the workspace provide quick access to common actions like submitting expenses or creating a calendar event. These actions are processed by your organizational systems through the integrations you've created in the Microapps service.

The **Actions** tab in the left navigation of the workspace displays all the actions available to subscribers with access to microapps. For example, these actions might include links to other organizational systems or intranet sites.

Customize workspace preferences

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

Allow Account Password to be Changed

Note:

This feature is being rolled out to customers incrementally. You might not see 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.

Allow Account Password to be Changed 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 Internet Explorer 11, or the latest version of Edge, Chrome, Firefox, or Safari web browsers.

This feature isn't supported on older versions of Workspace app and 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.

Add password requirements

1. From the Citrix Cloud menu, select **Workspace Configuration** and then select **Customize > Preferences**.
2. Under **Allow Account Password to be Changed**, check that the setting is enabled. If disabled, enable the setting.
3. Select **Add a password requirement**.

Allow Account Password to be Changed



When enabled, subscribers can change their password by going to "Security and Sign In" in Workspace.

Add the password requirements that are enforced by your organization's identity provider so your subscribers understand how to create valid, complex passwords. Workspace displays these requirements to your subscribers, but does not validate subscribers' passwords.

If no requirements are defined, subscribers see the message: **Your organization's password requirements still apply.**

[+ Add a password requirement \(20 max.\)](#)


Save

4. Enter a requirement that matches each of your organization's existing 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 that you want to show subscribers when they change their password.


Add a password requirement

Add the password requirements that are enforced by your organization's identity provider so your subscribers understand how to create valid, complex passwords. Workspace displays these requirements to your subscribers, but does not validate subscribers' passwords.

Password must meet the following requirements: ?

- 

[+ Add a password requirement \(20 max.\)](#)

 If no requirements are defined, subscribers see the message:
Your organization's password requirements still apply.

5. When you're finished adding requirements, select **Save**.

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

Allow Account Password to be Changed



When enabled, subscribers can change their password by going to "Security and Sign In" in Workspace.

^ Password must meet the following 4 requirements: ?

- At least 7 characters in length.
- Contain no personal information (Part of your name, social security number, birthday).
- Must contain 3 of the following: Lower Case Letter, Upper Case Letter, Number, Other Character (!@#% \).
- Must not be a password you have used before.



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 this 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**.

Change Password

You'll have to sign back in to Workspace after changing your password.

Current Password:

New Password:

Confirm Password:

▼ Hide Password Requirements

Passwords must meet the following requirements:

- Be at least ten (10) characters in length
- Contain an upper case letter
- Contain a lower case letter
- Contain a number
- Contain a symbol (e.g., !, @, \$, %...)
- Be different than the 24 previously reset passwords
- Do not include a common dictionary word
- Do not include any part of the user or login name
- Avoid padding passwords with consecutive or repetitive numbers (e.g. 123, 1234, 1111, etc.)

After changing their password, subscribers are automatically signed out of Workspace and must sign in again with their new password.

Add a custom subscriber license agreement policy

You can present subscribers with a custom usage agreement policy that they must read and accept before they sign into their Workspace. To configure this feature:

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. Enter a title for the policy under **Policy header**.
5. Enter the policy text that subscribers must agree to before logging in. If needed, add other languages in the same text box.

6. Enter the name of the button that subscribers must select to agree to the policy.

Sign In Policy ×

Define the company usage policy that your subscribers must read and accept before signing in and accessing resources. [Learn more](#)

Enable policy
When enabled, the policy will be displayed to end users.

☒

Policy header
Enter the header to display above the policy text.

Terms and Conditions

Policy text
Enter the text of the sign in policy you want to display to subscribers.


Normal ÷ **B** *I* U

Enter policy text

Button text
Enter the text to display for the button that will allow subscribers to continue to sign in.

Accept Terms and Conditions

Save Preview Cancel



7. Select **Preview** to see what the policy looks like for subscribers. Select **Close preview** to go back to the policy configuration.
8. When you're finished configuring the policy, 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.

Allow Caching

The **Allow Caching** setting enhances performance for subscribers accessing Workspace through a web browser. When caching is enabled, subscribers experience faster loading of their activity feed and can access resources in Citrix Files more quickly.

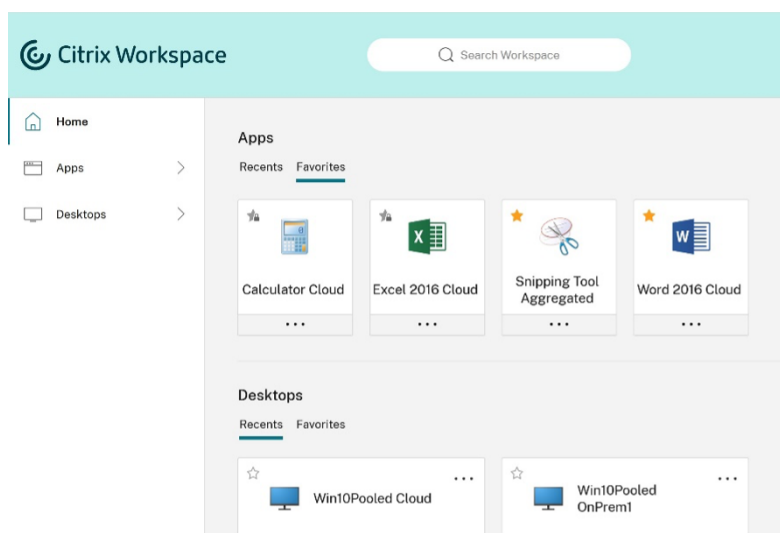
Caching is supported when accessing Workspace with a [supported web browser](#). Caching isn't available when using a locally installed Workspace app.

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 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 subscribers to favorite and unfavorite app and desktop resources. The **Allow Favorites** feature is enabled by default.

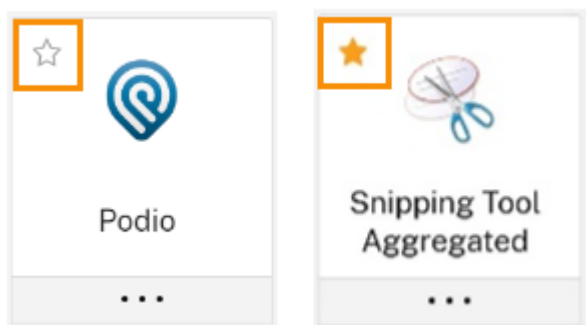


Note:

- For some existing customers (new to Workspace between December 2017 and April 2018), **Allow Favorites** defaults to **Disabled**. The administrator can decide when to enable this feature for their subscribers.
- **Allow Favorites** doesn't affect the ability to favorite files. The ability to favorite files persists

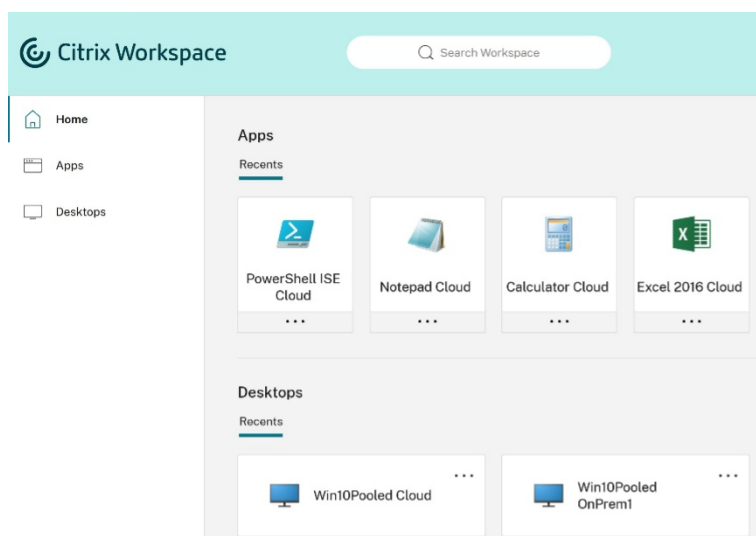
regardless of whether **Allow Favorites** is enabled or disabled in **Workspace Configuration**.

When enabled (default), workspace subscribers can add up to 250 favorites using the star icon at the top left-hand corner of each (non-mandatory) app and desktop card. The star changes from having no fill to a yellow fill when it is favorited.



If a subscriber favorites more than 250 resources, the “oldest favorite” is removed (or as close as possible to preserve the most recent favorites).

When disabled, workspace subscribers don’t see stars on app and desktop cards, or the **All Apps** and **Favorites** submenus for these resources in the navigation bar. App and desktop favorites aren’t deleted and can be recovered if you re-enable favorites.



App and desktop keywords

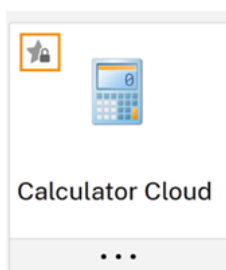
Administrators can automatically add favorite apps for subscribers by using **KEYWORDS:Auto** and **KEYWORDS:Mandatory** settings in the Virtual Apps and Desktops service (**Manage > Full Configuration > Applications**).

The screenshot shows the 'Application Settings' dialog box in Citrix Studio, with the 'Identification' tab selected. The left sidebar lists various settings: Identification, Delivery, Location, Groups, Limit Visibility, File Type Association, and Zone. The 'Identification' section contains the following fields:

- Application name (for user):** Calculator
- Application name (for administrator):** Calculator
- Description and keywords:** KEYWORDS: Auto

Below the description field, there is a note: "This is the description that will be seen by the user. You can also use this field to enter keywords for StoreFront." and a link to [Learn More](#). At the bottom right, there are three buttons: OK, Cancel, and Apply.

- **KEYWORDS:Auto.** The app or desktop is added as a favorite and subscribers can remove the favorite.
- **KEYWORDS:Mandatory.** The app or desktop is added as a favorite, and subscribers can't remove the favorite. Mandatory apps and desktops display a star icon with a padlock to indicate that it can't be unfavorited.



Note:

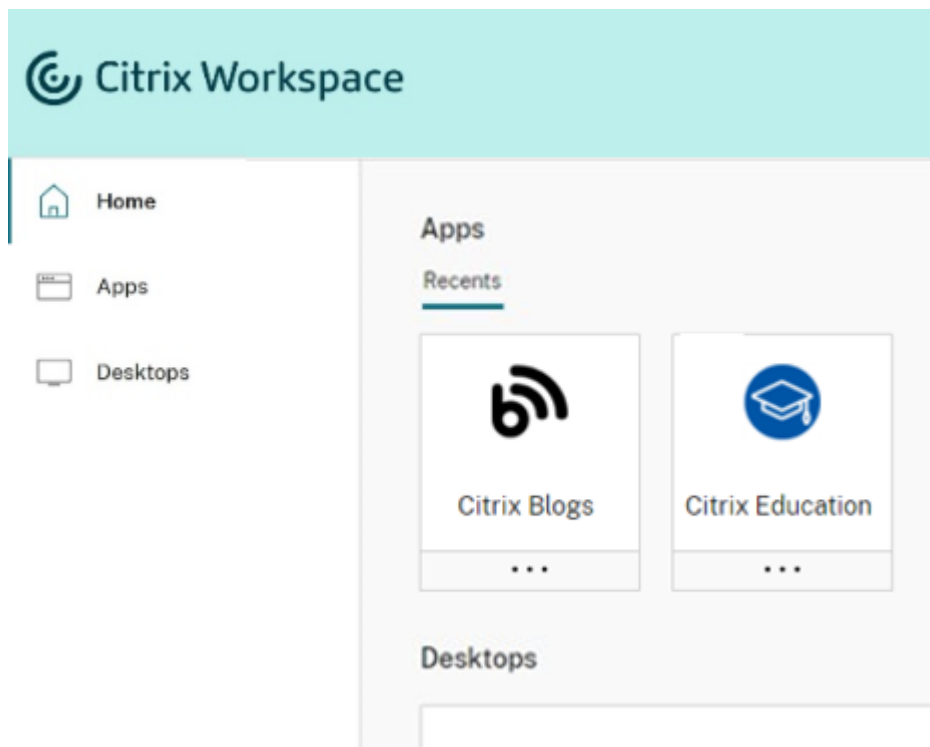
If you use both **Mandatory** and **Auto** keywords for an app, the **Mandatory** keyword overrides the **Auto** keyword, and the favorited app or desktop cannot be removed.

For a subscriber with access only to apps and desktops that have the **Mandatory** keyword:

- The subscriber sees only the Apps page in the left navigation pane in Workspace. The Favorites

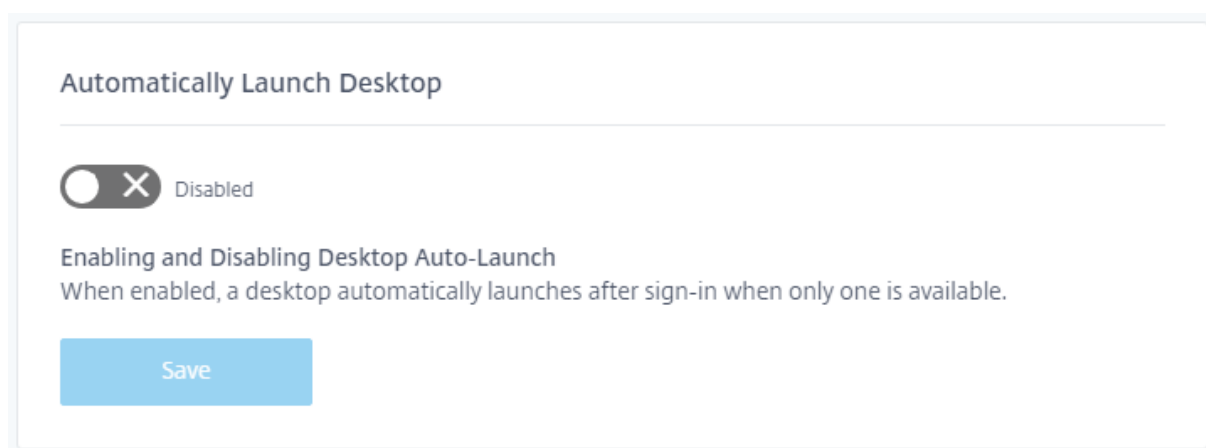
page doesn't appear in the left pane because there's no difference in the apps that appear on the Apps page and the Favorites page.

- The subscriber doesn't see the Favorites tab on the home page. Only the Recents tab is shown.



Automatically Launch Desktop

Automatically Launch Desktop is available to customers who have access to Workspace Configuration and the new workspace experience. This 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 the 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.

Inactivity Timeout for Web

Use the **Inactivity Timeout for Web** setting to specify the amount of idle time allowed (maximum of 8 hours) before subscribers are automatically signed out of Citrix Workspace. This setting applies to browser access only, and doesn't apply to access from a local Citrix Workspace app.

Workspace Sessions

Inactivity Timeout for Web

After this amount of idle time (maximum of 8 hours), your subscribers will be automatically signed out of Workspace. Applies to browser access only (not from a local Citrix Workspace app).

HOURS		MINUTES
0	▼	20 ▼

Unlike manual logout, which disconnects virtual app and desktop sessions, subscribers stay connected to their virtual app and desktop sessions following timeout due to inactivity.

Reauthentication period for Workspace app

Note:

This feature is available as a preview. Citrix recommends using preview features only in test environments or limited production environments.

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

Reauthentication Period for Workspace App ⓘ

This is the maximum time your subscribers can stay signed in to Workspace app before needing to reauthenticate (between 1 and 365 days).

Current Reauthentication Period: 1 Day(s) [Edit](#)

[Learn more](#) about Workspace reauthentication periods.

Save

The default for accounts provisioned after September 27, 2021, requires subscribers to sign in every 30 days. The default for accounts provisioned before this date will continue to be 1 day (24 hours).

You can specify any reauthentication period of up to 365 days. Reauthentication periods that are longer than the default require subscribers' consent to stay signed in.

If you change the reauthentication period length, the change takes about 10 minutes to take effect. During that time, subscribers aren't able to access their workspace.

During the reauthentication period that you set, subscribers stay logged in unless they're inactive for 4 or more days at a time. If a subscriber is inactive for 4 or more days, they are prompted to reauthenticate the next time that they attempt to access their workspace.

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 Workspace app is supported for the following authentication methods:

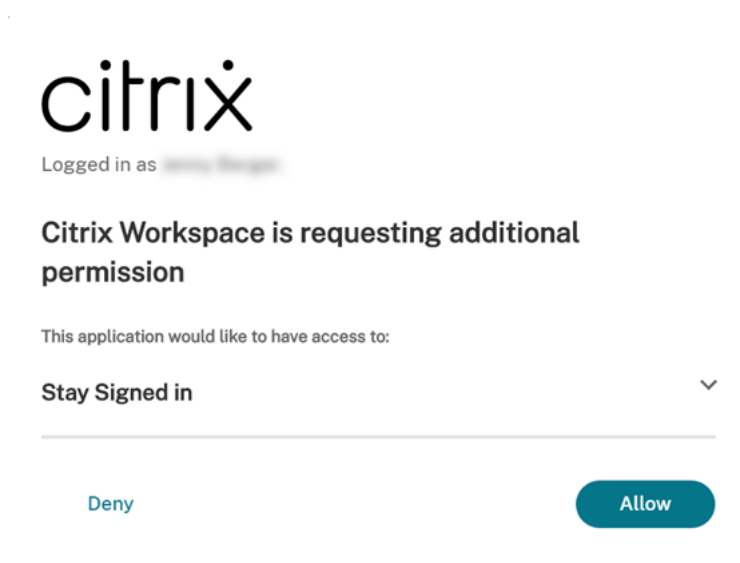
- Active Directory
- Active Directory plus token
- Azure Active Directory
- Citrix Gateway
- Okta

Staying signed in to Virtual Apps and Desktops sessions is supported for the following authentication methods:

- Active Directory
- Active Directory plus token
- Citrix Gateway

Subscriber experience for staying signed in

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

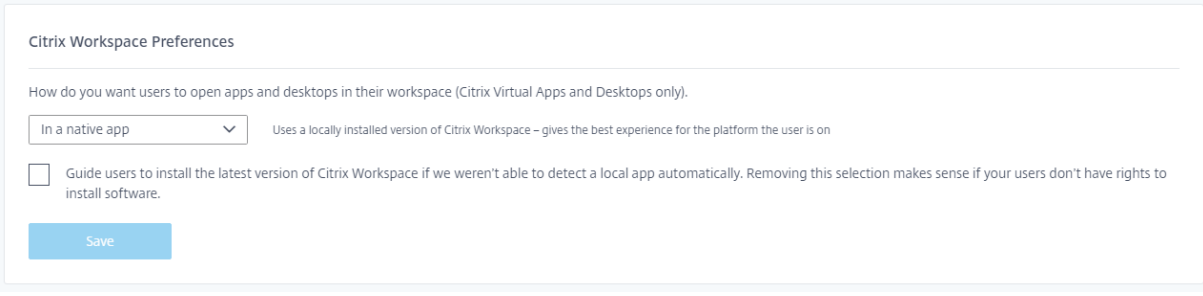


When the subscriber selects **Allow**, they stay signed in for the duration of the reauthentication period. If no activity is detected on a subscriber's device for four days, the subscriber is automatically prompted to reauthenticate. After they sign in to the Workspace app, the reauthentication period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

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

Opening Apps and Desktops

The **Opening Apps and Desktops** setting is available to customers who have access to Workspace Configuration and the new workspace experience. This preference applies to the way users open apps and desktops delivered by Citrix Virtual Apps and Desktops only (service, or on-premises from the [Site aggregation](#) feature). It doesn't apply, for example, to SaaS apps delivered by the Citrix Gateway service. This preference is available to new and existing customers. However, the introduction of this feature doesn't change any settings for existing customers.



The screenshot shows a 'Citrix Workspace Preferences' dialog box. It contains a title bar, a subtitle 'How do you want users to open apps and desktops in their workspace (Citrix Virtual Apps and Desktops only).', a dropdown menu set to 'In a native app', a checkbox labeled 'Guide users to install the latest version of Citrix Workspace if we weren't able to detect a local app automatically. Removing this selection makes sense if your users don't have rights to install software.', and a 'Save' button at the bottom.

Choose one of the following settings:

- **In a native app** (default). Uses a locally installed version of Citrix Workspace. This gives the best experience for the platform the subscriber is on.
- **In a browser**. Uses Citrix Workspace for HTML5. No client software is required.
- **Let users choose**. Prompts subscribers to detect a locally installed version of Citrix Workspace, or to use Citrix Workspace for HTML5 in their browser where possible.

There's an additional option for the **In a native app** and **Let users choose** settings to guide users to install the latest version of Citrix Workspace if a local app isn't detected automatically. Removing this selection makes sense if your users don't have rights to install software.

Integrate Microsoft Teams with Workspace

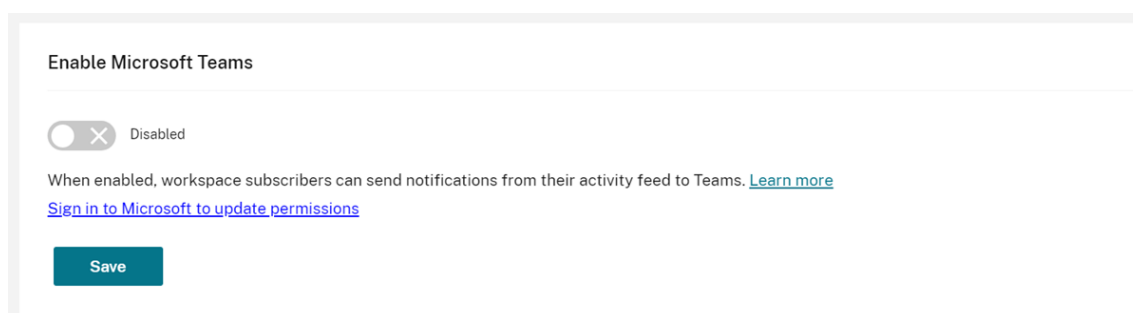
With the Microsoft Teams integration, subscribers can share cards from their workspace Activity feed with other subscribers through channels in Microsoft Teams.

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**. 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. For more information about configuring Azure AD authentication, see [Connect Azure Active Directory to Citrix Cloud](#).
- You must have Microapps enabled in your Citrix Cloud account. For more information about enabling Microapps, see [Getting started](#).
- The feature toggle **lwsMicrosoftTeams** must be enabled. Contact your Citrix Cloud administrator for more information.
- You must have the **Actions and Activity Feed** feature enabled for workspaces.
- Workspace subscribers have the Microsoft Teams desktop client installed.

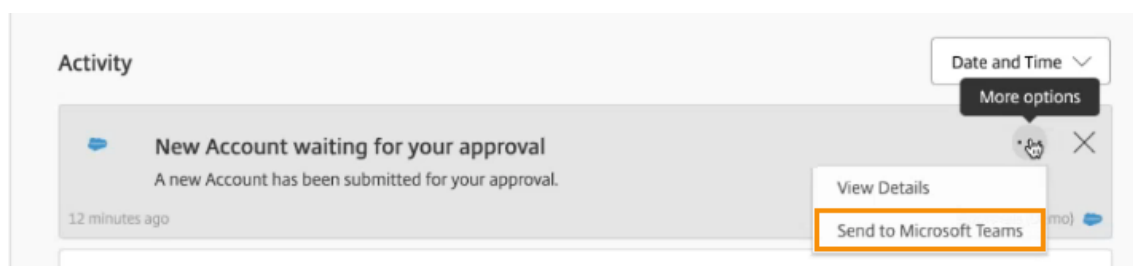
Enable Microsoft Teams integration

1. After signing in to Citrix Cloud, select **Workspace Configuration** from the menu.
2. Select **Customize**, and then the **Preference** tab.
3. Under **Enable Microsoft Teams**, select the toggle to enable. The toggle turns green when the integration is successfully enabled.



4. Select **Save**.

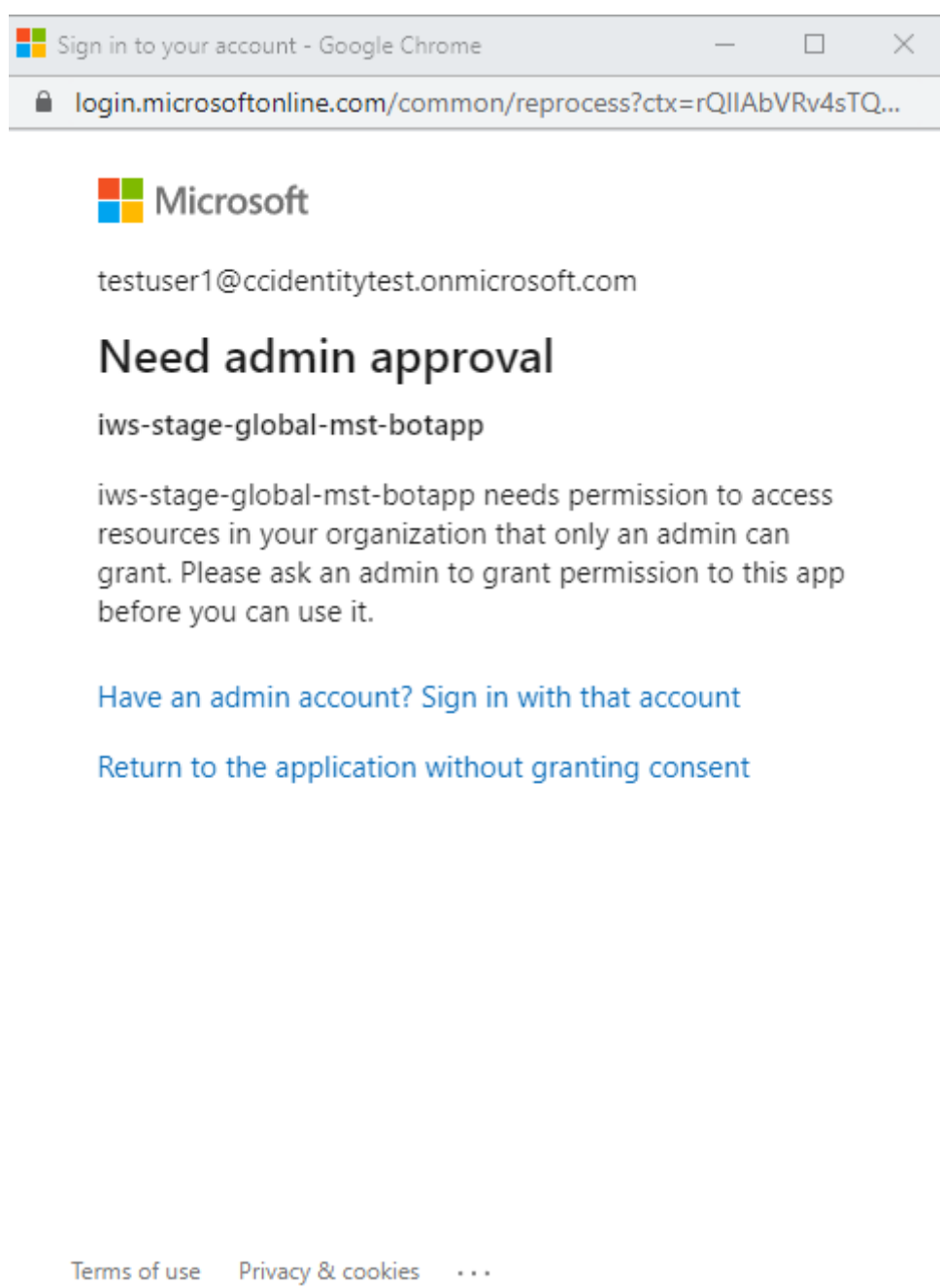
Workspace users can now see the **Send to Microsoft Teams** option and share cards from Workspace. Users may need to refresh their screens (Ctrl+F5).



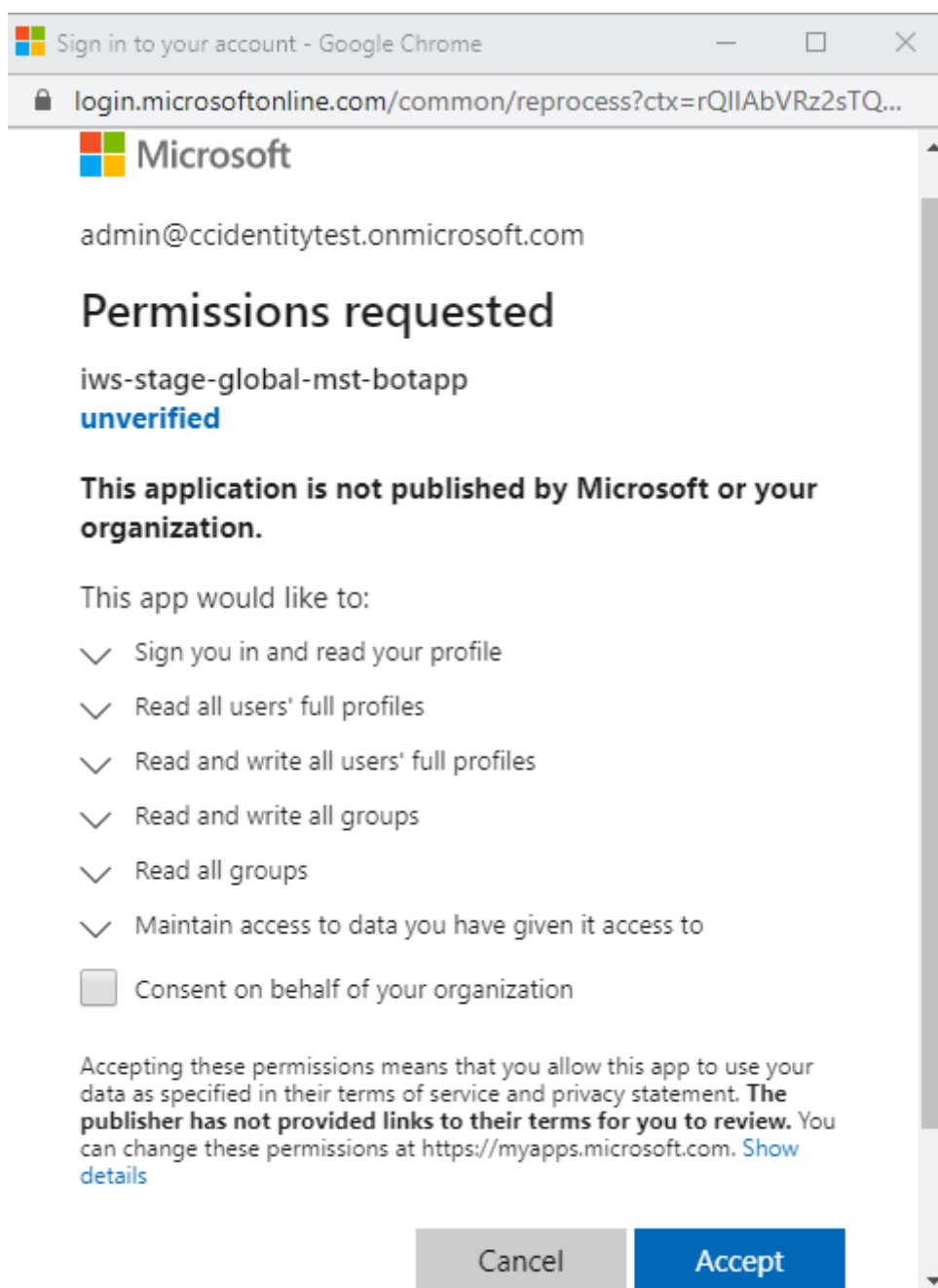
Accept Workspace permissions

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



2. To accept permissions, log 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:



3. 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.
4. Select **Accept**.

Aggregate on-premises virtual apps and desktops in workspaces

September 9, 2021

If you have an on-premises Virtual Apps and Desktops deployment, you can add your Site to Citrix Workspace to make your existing apps and desktops available to subscribers. This process is known as *Site aggregation*. 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.

Note:

This feature is included in all Citrix Workspace editions. For more information about the features included in each Workspace edition, see the [Citrix Workspace Feature Matrix](#).

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
- XenApp 6.5

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 which are End of Life. XenApp and XenDesktop Current Releases before 7.14 reached End of Life on June 30, 2018. Support for Workspace Site aggregation with End of Life versions of XenApp and XenDesktop 7.x depends on successful enumeration and launch of resources with your StoreFront deployment.

XenApp 6.5 reached End of Life on June 30, 2018. Support for Workspace Site aggregation with End of Life versions of XenApp depends on successful enumeration and launch of resources in your StoreFront or Web Interface on-premises deployment.

To use Site aggregation with an on-premises deployment that includes the Citrix Federated Authentication Service (FAS), you must meet the following requirements:

- Your on-premises Site uses one of the following Citrix product versions:
 - Virtual Apps and Desktops 7 1808 or later
 - XenApp and XenDesktop 7.16 through 7.18
- Your FAS servers are updated to the latest version of the FAS software which connects to Citrix Cloud. Connecting to Citrix Cloud is required to use FAS with Citrix Workspace. For more information, see [Enable single sign-on for workspaces with Citrix Federated Authentication Service](#).

Task overview

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

- Discover your Site and select the default resource location. The default resource location specifies the domain and connectivity method for all users who access your Site. During this process, Citrix Cloud performs a connectivity test to verify that your Site is reachable and displays your resource locations. If you have resource locations with no Cloud Connectors installed, you can download and install the required software.
- Detect the Active Directory domains in which your Cloud Connectors are installed. For XenApp 6.5, Citrix Cloud also detects if there are any published applications assigned to local user accounts on XenApp servers. To use Citrix Workspace, application users must authenticate with Active Directory. Citrix Cloud provides a list of any local user accounts detected so you can ensure they can authenticate to Citrix Workspace.
- Specify the connectivity you want to use between Citrix Cloud and your Site. For external connectivity, you can use your own Citrix Gateway or use the Citrix Gateway service. To ensure only users on the same network as your Site can access applications, you can specify internal-only access.

Prerequisites

Cloud Connectors

You need at least two (2) servers on which to install the Citrix Cloud Connector software. These servers must meet the following requirements:

- Meets the system requirements described in [Cloud Connector Technical Details](#).
- Doesn't have any other Citrix components installed, isn't an Active Directory domain controller, and isn't a machine critical to your resource location infrastructure.
- Joined to the domain where your Site resides. If users access your Site's applications in multiple domains, you must install at least two Cloud Connectors in each domain.
- Connected to a network that can contact your Site.
- Connected to the Internet. For more information, see [System and Connectivity Requirements](#).
- Citrix recommends two servers for Cloud Connector high availability. After installation, the Cloud Connectors allow Citrix Cloud to locate and communicate with your Site.

For more information about installing the Cloud Connector, see [Cloud Connector Installation](#).

Citrix recommends installing the Cloud Connectors before adding your Site to Citrix Workspace to ensure that your Site is added with minimal interruption.

Web proxy configuration

If you have a web proxy in your environment, you must ensure that the Cloud Connectors can validate connectivity to the XML Service in your Site. To do this, add each XML server to the bypass proxy list on each Cloud Connector. Don't use wildcards; the Cloud Connector supports handling FQDNs only.

1. Add the XML servers to the bypass proxy list:
 - a) On the Cloud Connector, click **Start** and then type **Internet Options**.
 - b) Select the **Connections** tab and then select **LAN Settings**.
 - c) Under **Proxy server**, click **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 the Cloud Connector services can consume them appropriately. 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. Alternatively, restart each machine.

Active Directory

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

Azure Active Directory configuration

To allow Sites using Azure Active Directory to be added to Citrix Workspace, you must 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](#).
- For XenApp 6.5, see [Configuring the Citrix XML Service Port and Trust](#).

Important:

If you choose to use Azure Active Directory authentication with Site aggregation, users are prompted to authenticate to each application they launch.

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. When you add your 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:

- You can't use separate user and resource forests when you define the default resource location during the process of adding your Site. Because the 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 aren't able to use Citrix Workspace after an on-premises Site is added through Site aggregation. Only users located in the forests that the Site trusts can log in and use Citrix Workspace. If users from an untrusted forest attempt to log 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. To use this option, 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 if you prefer 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 while adding your Site to Workspace, you must use the same OrgID that 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 ensures the Controller that you specify is available. Before you add your on-premises Site, perform the following tasks:

- Ensure you have Citrix administrator credentials with a minimum of Read Only permissions. During the process of adding your Site to Citrix Workspace, Citrix Cloud prompts you to supply these credentials. Citrix Cloud only reads these credentials for the discovery process. Citrix Cloud doesn't store these credentials or use them to make changes to your Site.
- **XenApp 6.5 only:** Ensure that port 2513 on the XenApp server is accessible from the Cloud Connector machines in your environment. During the discovery process, the Cloud Connectors contact the Citrix XenApp Remoting Service on the XenApp server you specify. This service listens on port 2513. If this port is blocked, Citrix Cloud can't discover your deployment.

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 your Site credentials for security reasons, you can enable 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 your Site

In this step, you provide the information that Citrix Cloud needs to locate your Site and select your default resource location. The default 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, click **Workspace Configuration** and then click **Sites > Add Site**.
2. In **Select type of Site**, select the XenApp or XenDesktop version of the Site you want to add. Citrix Cloud attempts to discover any Cloud Connectors in your domain and displays them in the next tab.
3. In **Discover XenApp Site** or **Discover XenApp and XenDesktop Site**, perform one of the following actions:
 - a) If you have no Cloud Connectors installed in your Site's domain, click **Install Connector**. Citrix Cloud prompts you to download the Cloud Connector software and complete the installation wizard.
 - b) If you have Cloud Connectors installed, Citrix Cloud displays the connectors in the domains in which they were detected. Select the resource location you want to add to Citrix Workspace. This resource location becomes the default resource location.
 - c) If you have Cloud Connectors installed, but they aren't displayed, click **Detect**.

4. In **Enter Server Address**, enter the IP address or FQDN of a Controller in the Site.
5. **XenApp 6.5 only:** Enter the port for the XML Server. If the XML Server port uses SSL, select **Use SSL**.

Note:

For XenApp and XenDesktop 7.x Sites, Citrix Cloud automatically discovers the XML server port.

6. Click **Discover**.
7. If prompted, type the Citrix Administrator credentials for the Site and click **Continue**. Citrix Cloud performs a connectivity test to verify that your Site is reachable. Discovery might take a few minutes to complete, depending on the type and size of the Site.
8. Click **Continue**.

Task 2: Verify Active Directory Connection

In **Verify Active Directory Connection**, Citrix Cloud displays the domains used with your Site and whether or not there are Cloud Connectors installed in those domains. For XenApp 6.5, Citrix Cloud also displays an alert if there are any local user accounts on the XenApp servers assigned to any applications.

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 only one Cloud Connector is installed, your Site's connection to Citrix Cloud is at risk of an outage, preventing users from using Citrix Workspace. To ensure high availability for your Site, Citrix recommends installing at least two (2) Cloud Connectors in each domain.

XenApp 6.5: If there are local user accounts assigned to published applications, these users must be assigned to applications using their Active Directory account instead. Otherwise, they can't use Citrix Workspace to access their applications. Citrix Cloud provides a downloadable list in CSV format of the applications and the local user accounts assigned to them.

1. To install more Cloud Connectors, click **Install Connector**. If your domain has only one Cloud Connector and you choose to continue without installing more Cloud Connectors, select **I understand that high availability requires having two connectors installed in each domain**.
2. If you have local users assigned to applications in your Site, click **Download user list (.csv)**.
3. Click **Continue**.

Task 3: Configure connectivity and confirm settings

In this step, you specify whether you want to allow only external user access or internal-only access to your Site through Citrix Workspace. Internal connectivity requires your users to be on the same

network as your Site. For external connectivity, you can use your existing Citrix Gateway or you can use the Citrix Gateway service.

1. In **Configure Connectivity**, under **Select connectivity type**, select one of the following options:
 - **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 use your existing subscription with your Site.
 - **Internal Only:** If selected, no other configuration is needed. Click **Continue**.
2. If **Add Existing Gateway** is selected, perform the following actions:
 - a) Click **Edit** and type the public URL of the Citrix Gateway.
 - b) Verify that Citrix Gateway is configured to use your Cloud Connectors as the STA servers as described in [CTX232640](#).
 - c) Click **Test STA**. When the test is successful, click **Continue**. If the test isn't successful, refer to [CTX232517](#) for troubleshooting steps.
3. 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, click **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, if applicable.
4. Click **Continue**.
5. In **Confirm Site Aggregation**, review the XML port, XML servers, Active Directory domains, and the Connectivity Type you chose earlier.
6. Click **Save and Finish**. The Sites page displays your newly added Site.

Notes:

- Citrix Cloud displays up to five of the XML servers with which it can connect. If you have multiple XML servers in your Site but only one is displayed, Citrix Cloud displays an alert. To troubleshoot this issue, refer to [CTX232516](#).
- If you want to specify different XML servers, click **Save and Finish**. You can then edit your Site to change these values.

Change your Site configuration

Rediscover your Site

If you add Delivery Controllers to your Site or change XML ports, you can initiate rediscovery to verify that your Site is still reachable in Citrix Workspace.

1. On the **Sites** page, click the ellipsis button for the Site you want to update and click **Edit Site**.
2. In **Server Address**, type the IP address or FQDN of a Delivery Controller in your Site and click **Rediscover**.

Add or modify XML servers

When you add a new Site to Citrix Workspace, Citrix Cloud automatically detects XML servers in your Site and displays up to five XML servers in your Site 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. On the **Sites** page, click the ellipsis button for the Site you want to update and click **Edit Site**.
2. In the **XML Servers** section, type 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 in which they appear in the list. You can reorder the list by dragging and dropping each server as needed.
4. Click **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 only, one IP range for machines in the EU where users connect through your existing Citrix Gateway, and one IP range for machines in the US where users connect through the Citrix Gateway service.

1. On the **Sites** page, click the ellipsis button for the Site you want to update and click **Edit Site**.
2. In the **Connectivity** section, click **Add an IP range with a different connectivity option**.
3. Type an IP range in CIDR format.
4. To create a new resource location for your IP range, perform the following actions:
 - a) Select **Add a new Resource Location** and type a friendly name.
 - b) In **Select your connectivity**, select whether you want to provide internal-only access or allow external access using your existing Citrix Gateway or the Citrix Gateway service.
5. To assign an existing resource location to the IP range, choose **Select an existing resource location** and then select the resource location you want to use. 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**.
6. Click **Add**.

Add more Active Directory domains

If you install Cloud Connectors in additional domains with Active Directory users in your Site, you can ensure they're added to your Site configuration in Citrix Workspace.

1. On the **Sites** page, click the ellipsis button for the Site you want to update and click **Edit Site**.
2. Under Active Directory, click **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 you can disable all on-premises Sites you've added to Citrix Workspace.

When Sites are disabled, users can no longer access the on-premises applications in those Sites through Citrix Workspace. However, the configuration for those Sites is preserved. When you re-enable a Site later on, the Site's default resource location, domain, XML server, and connectivity settings are retained.

To disable an on-premises Site

1. On the **Sites** page, click the ellipsis button for the Site you want to disable.
2. Click **Disable**. A confirmation message appears.
3. Click **Disable**.

To disable all on-premises Sites

To disable all Sites on the Sites page, you disable the workspace integration for all Virtual Apps and Desktops on-premises Sites. Disabling the workspace integration effectively disables Site aggregation of on-premises Sites. For instructions, see [To disable workspace integration for a service](#).

To re-enable any individual on-premises Sites or to add a new Site later on, you must first re-enable the workspace 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 make any changes to your Site.

1. On the **Sites** page, click the ellipsis button for the Site you want to remove.
2. Click **Delete**.

Enable single sign-on for workspaces with Citrix Federated Authentication Service

June 30, 2021

Citrix Federated Authentication Service (FAS) supports single sign-on to virtual apps and desktops in Citrix Workspace. 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:

- **FAS servers connected with a single resource location:** If your resource locations contain varied infrastructure (for example, different resource locations contain different Active Directory forests (AD forests), you deploy FAS servers to the same resource location where your VDAs reside. Single sign-on 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 (for example, they reside within a single AD forest), you can connect your FAS servers with multiple resource locations. Single sign-on is active for workspace subscribers who connect to virtual apps and desktops in those resource locations. In this scenario, there's no need to connect separate FAS servers to each resource location.

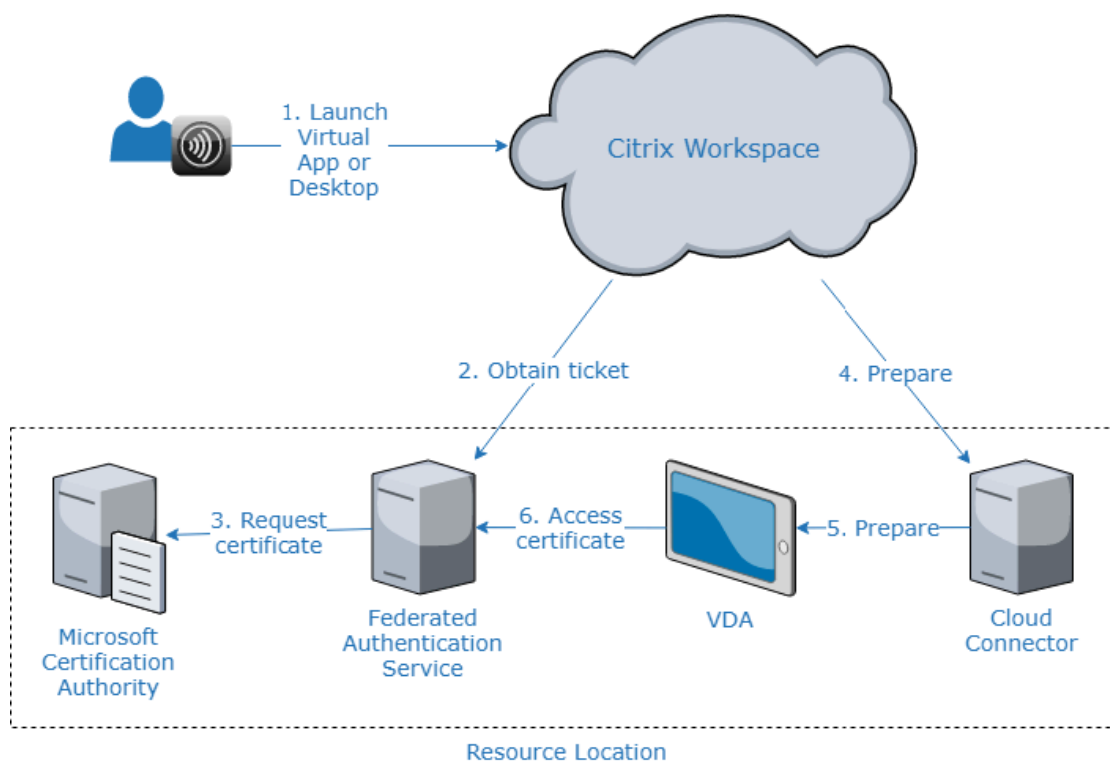
Note:

Using FAS with multiple resource locations is currently available as a preview feature. Citrix recommends using preview features only in test environments or limited production environments.

In both scenarios, subscribers signing in to their workspaces through a federated identity provider (such as Azure AD, Okta, SAML, and so on) enter their credentials only once to access their apps and desktops.

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.



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 single sign-on for workspaces with FAS, the FAS administration console and FAS service access the following addresses using the console user's account and the 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

If your environment includes proxy servers, configure the user proxy with the addresses for the FAS administration console. Also, ensure 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. 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-premise deployments.

Citrix Workspace

You must have the Citrix Virtual Apps and Desktops service provisioned and enabled in Workspace. By default, the Virtual Apps and Desktops service 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 reside) 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 is not an Active Directory domain controller, and is not a machine critical to your resource location infrastructure.
- Joined to the domain where your VDAs reside.

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 are 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, add the FAS server as described 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 are not required.

Tip:

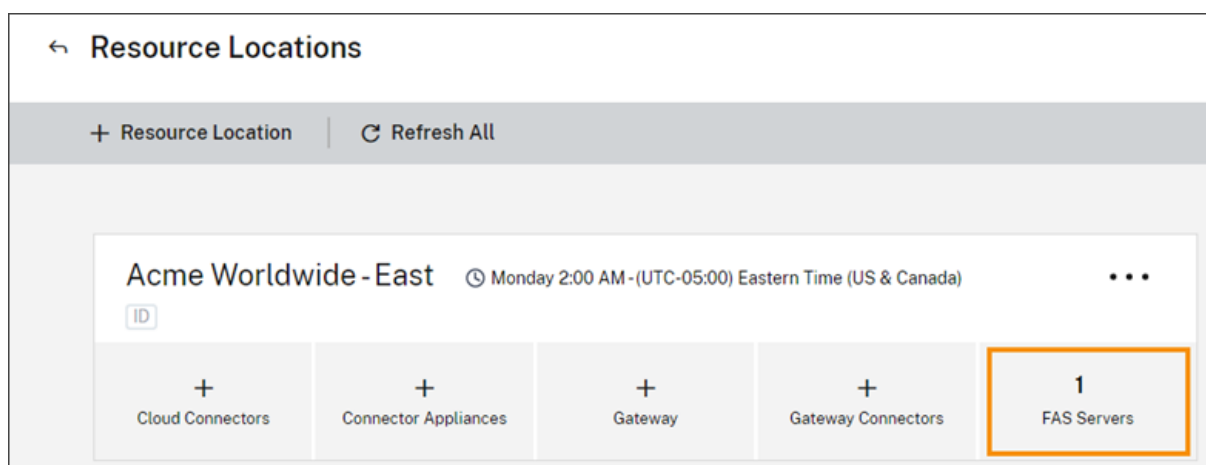
You can also download the Federated Authentication Service installer from the Citrix Cloud console:

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.

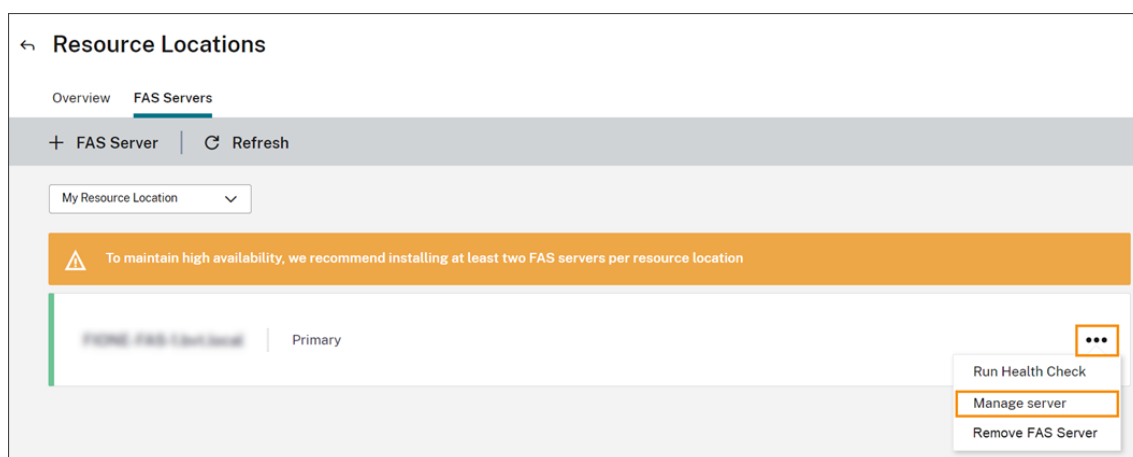


If you already have the Resource Locations page loaded in your browser, refresh the page to display the registered FAS server.

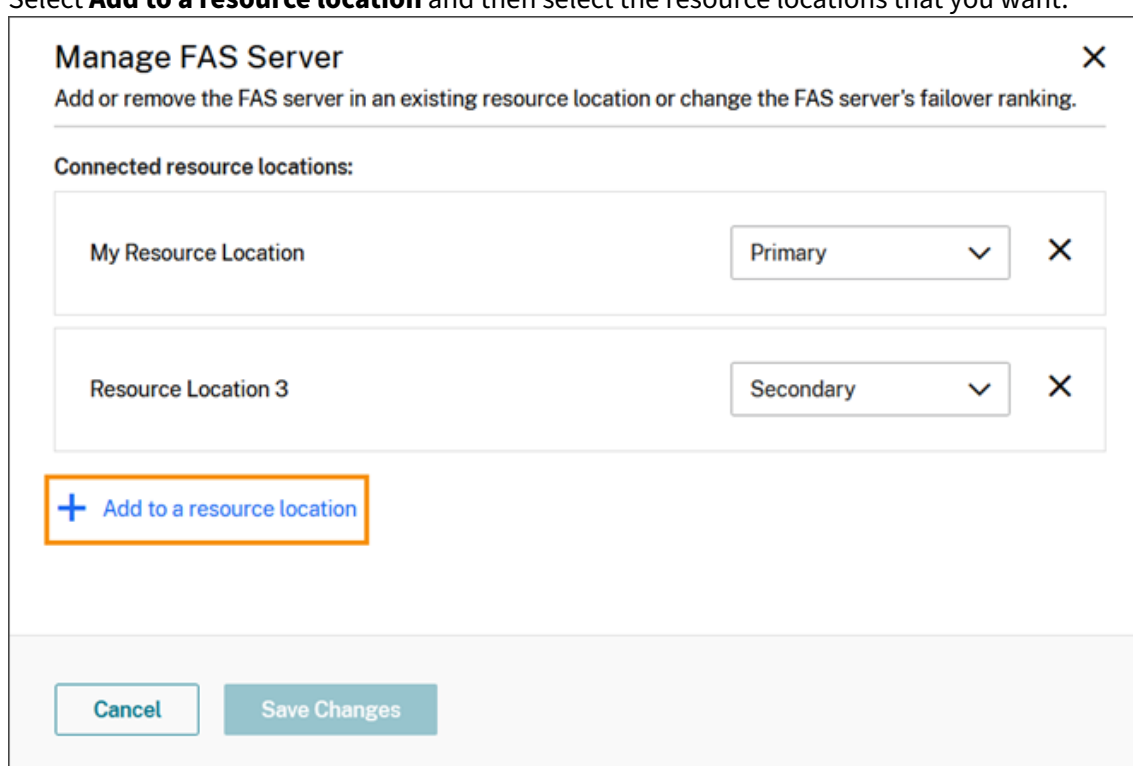
Add a FAS server to multiple resource locations

This feature is available as a preview. Citrix recommends using preview features only in test environments or limited production environments.

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 dropdown list.

Change a FAS server's failover priority

When subscribers launch a virtual app or desktop, Citrix Cloud uses the following sequence to select a FAS server in the same resource location as the app or desktop that is being launched:

- 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.
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 dropdown list.

Manage FAS Server ✕

Add or remove the FAS server in an existing resource location or change the FAS server's failover ranking.

Connected resource locations:

My Resource Location	Primary ▼	✕
Resource Location 3	Secondary ▼	✕

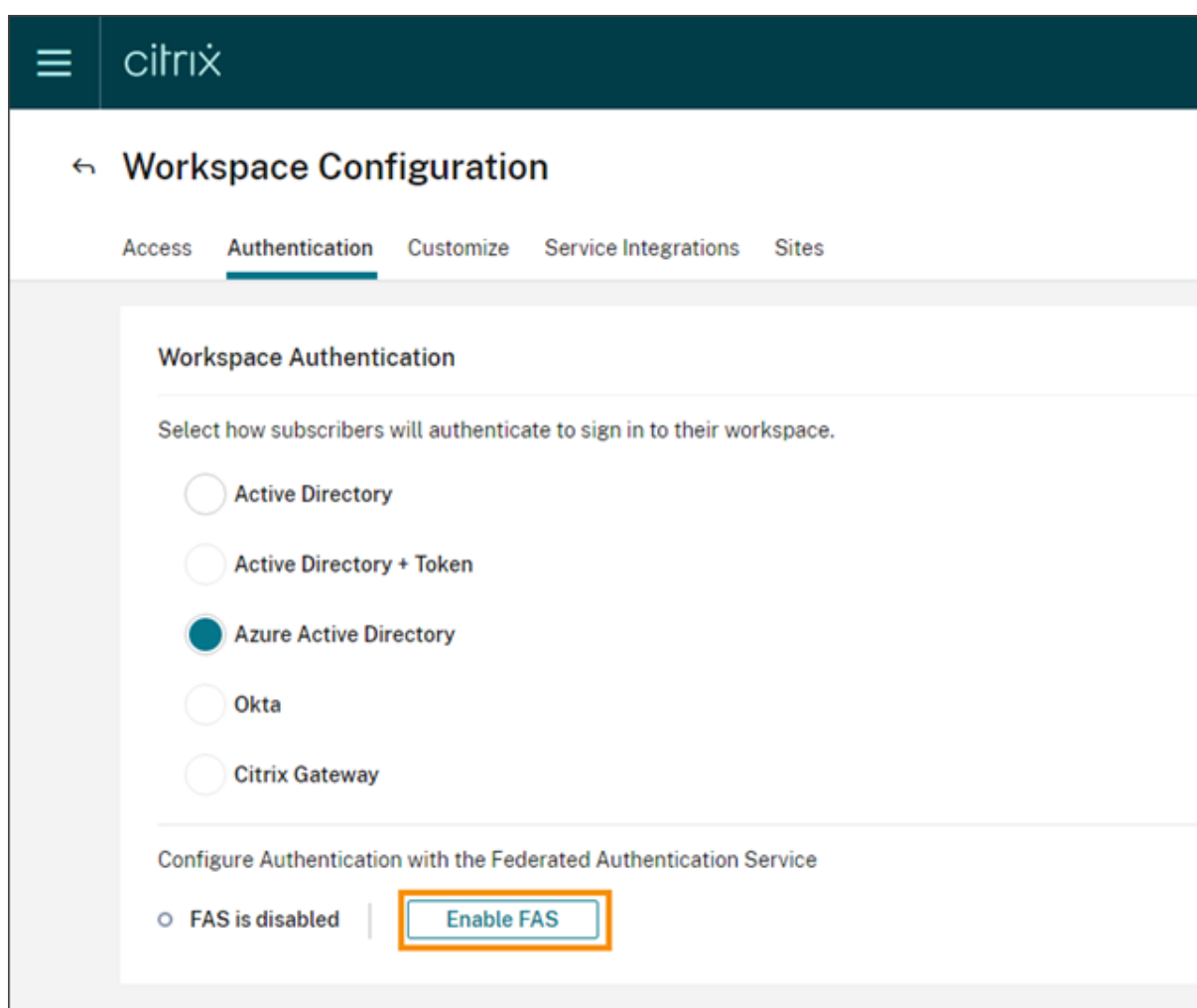
+ Add to a resource location

Cancel Save Changes

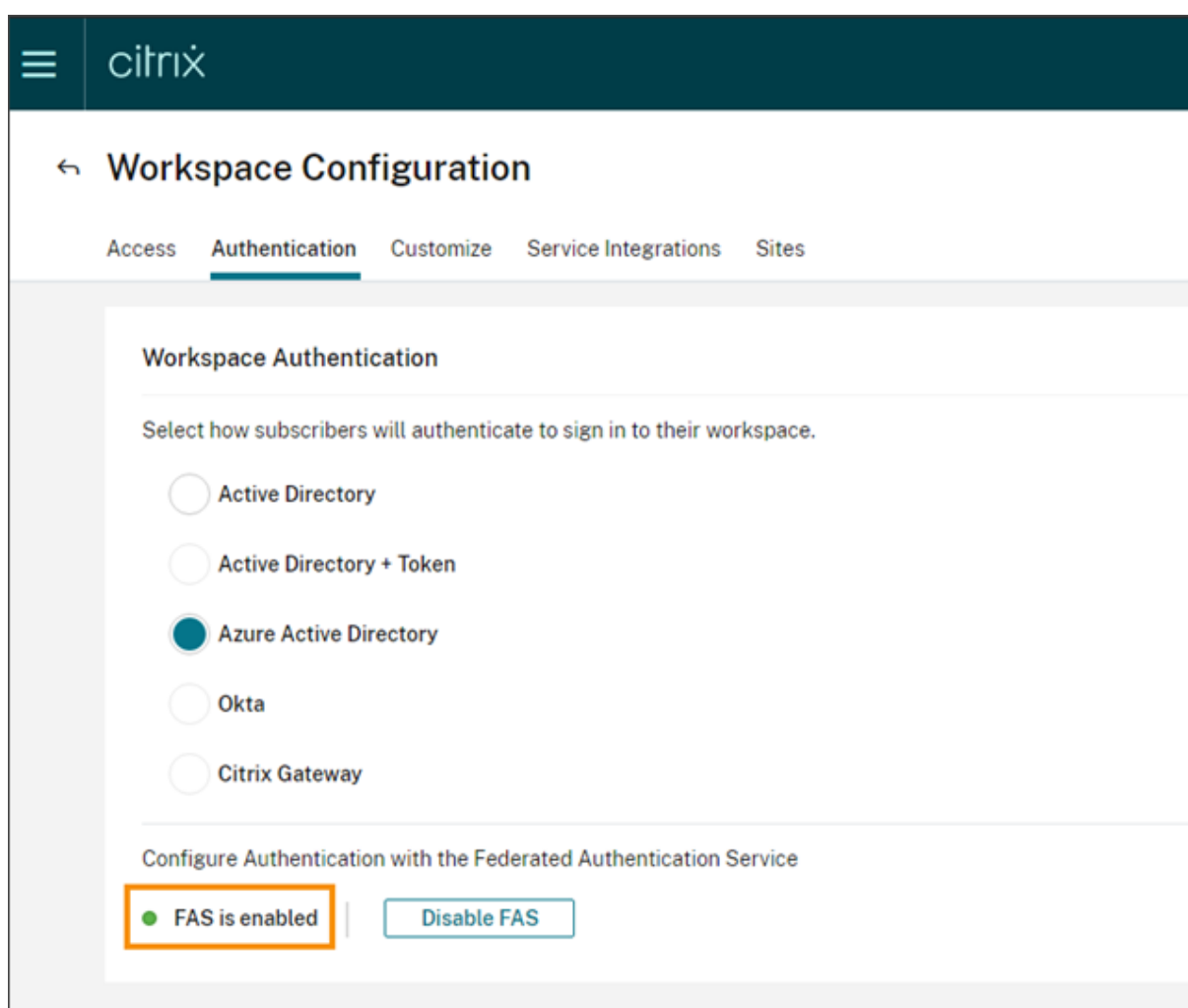
5. Select **Save Changes**.

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 is not 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

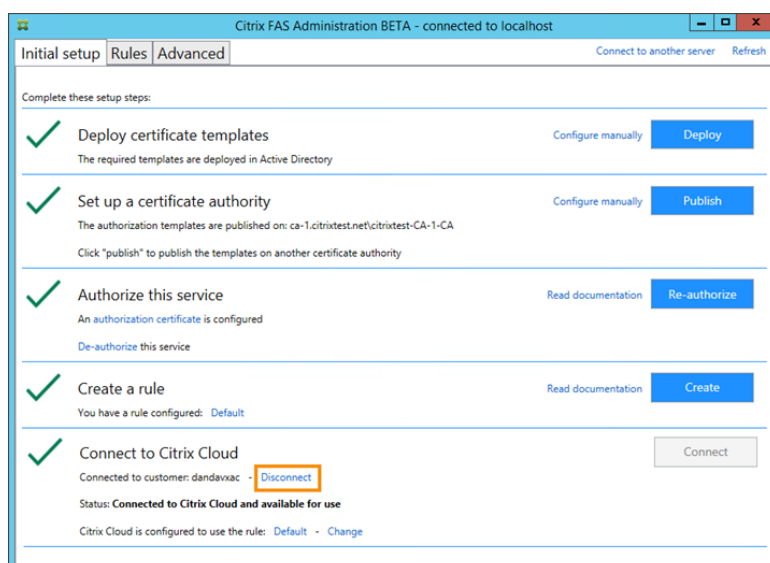
then select **Manage server**.

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:

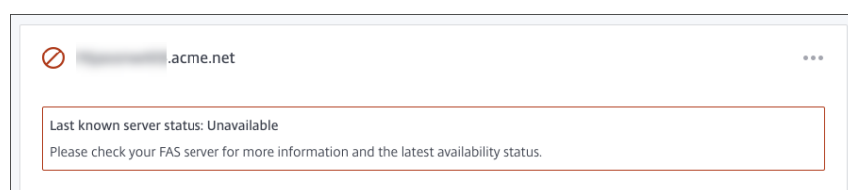
1. From the Citrix Cloud menu, select **Resource Locations**.
2. Locate the resource location you want to manage and then select the **FAS Servers** tile.
3. Locate the FAS server you want to remove, click the ellipsis at the right side of the entry, and then select **Remove FAS Server**.

4. On the FAS administration console (on your on-premises FAS server), in **Connect to Citrix Cloud**, select **Disconnect**. Alternatively, you can uninstall FAS.

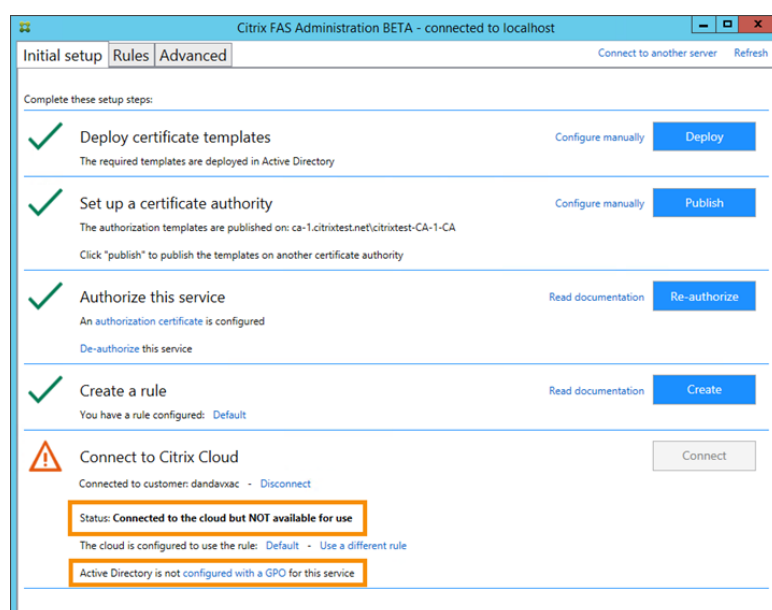


Troubleshooting

If the FAS server is not 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 is not 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](#).

Optimize connectivity to workspaces with Direct Workload Connection

July 7, 2021

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. 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 the VDAs in your environment with 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 networks from which virtual apps or desktops are launched in Workspace 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 Citrix Gateway. If a subscriber connects externally, Citrix Cloud routes them through Citrix Gateway, then redirects the subscriber through the Citrix Cloud Connector to the VDA in the internal network.

Important:

If your environment includes Citrix Virtual Apps and Desktops Standard for Azure alongside on-premises VDAs, configuring Direct Workload Connection causes launches from the internal network to fail.

Secure Browser, Citrix Virtual Apps Essentials, and Citrix Virtual Desktops Essentials 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

Virtual Apps and Desktops 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 will fail as Workspace tries to route internal users directly to the VDA, which isn't possible.

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.
- The Virtual Apps and Desktops service is enabled in **Workspace Configuration > Service Integrations**.
- You're using on-premises VDAs to deliver virtual resources to workspace subscribers.

Enable TLS for Workspace app for HTML5 connections

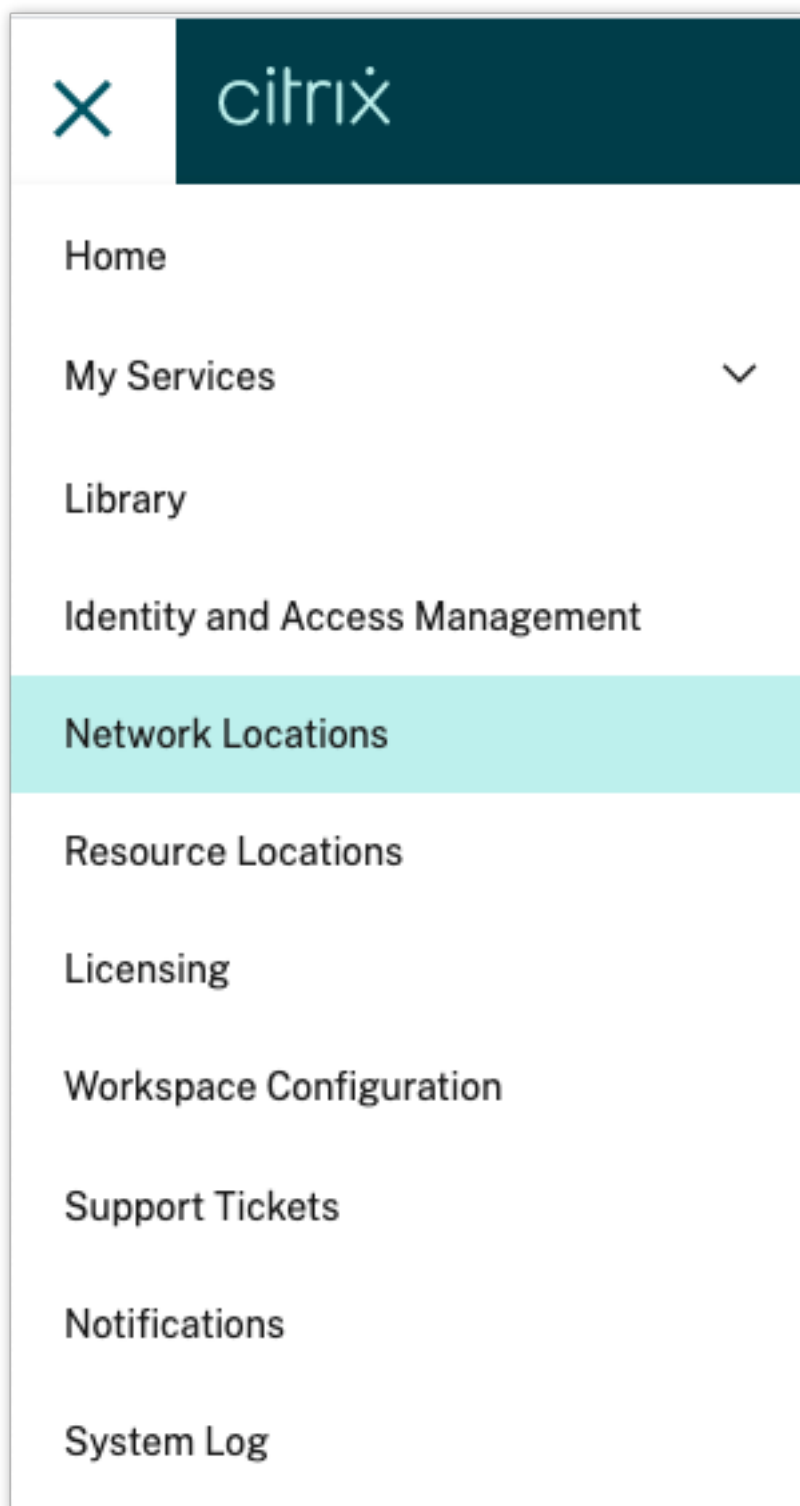
If your subscribers use Citrix Workspace app for HTML5 to launch apps and desktops, Citrix recommends that you have TLS enabled on the VDAs in your internal network. TLS ensures direct connections to VDAs. If VDAs don't have TLS enabled, app and desktop launches are routed through the Gateway when subscribers 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.

Citrix Cloud network location configuration

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.

Create a network location

1. In the Citrix Cloud console, navigate to **Network Locations** from the main menu.



2. Select the **Add network location** button in the top right-hand corner.

←

Network Locations

Network locations work with certain Workspace settings to enhance subscribers' experience across Citrix Cloud services.

Search...

Q

Add network location

Location name ↓	Public IP address range	Location tags	
Raleigh, NC		HQ, CCC, WS	...

3. Enter a network location name, public IP address range for the location, and location tags.

Add Network Location ×

Location name

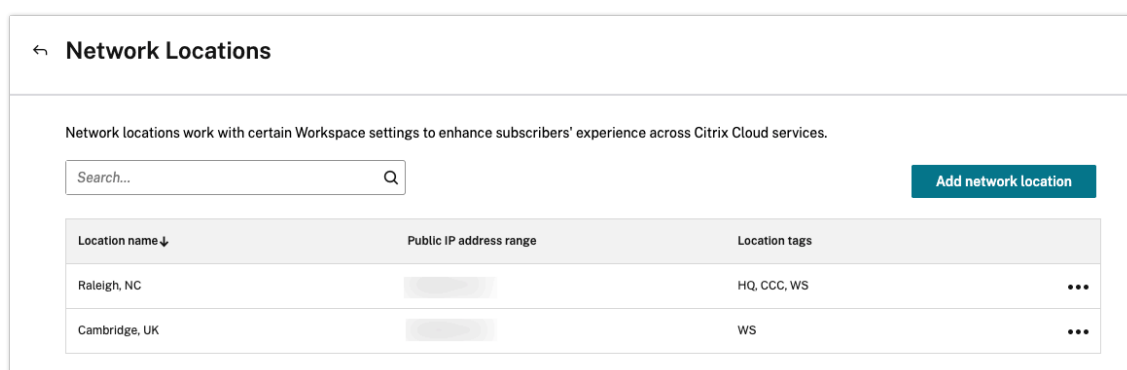
Public IP address range

Location tags

 ?

Save

4. Repeat these steps for each new network location you want to add.



Modify or remove network locations

1. In the Citrix Cloud console, navigate to **Network Locations** from the main menu.
2. Select the ellipses next to the network location that you want to modify or remove and then either:
 - Select **Edit** to modify a network location and then **Save** your changes to see them in the network locations page; or
 - Select **Delete** to remove a network location. You're asked to confirm this decision before the network location is deleted. You can't undo this action.

PowerShell network location configuration

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

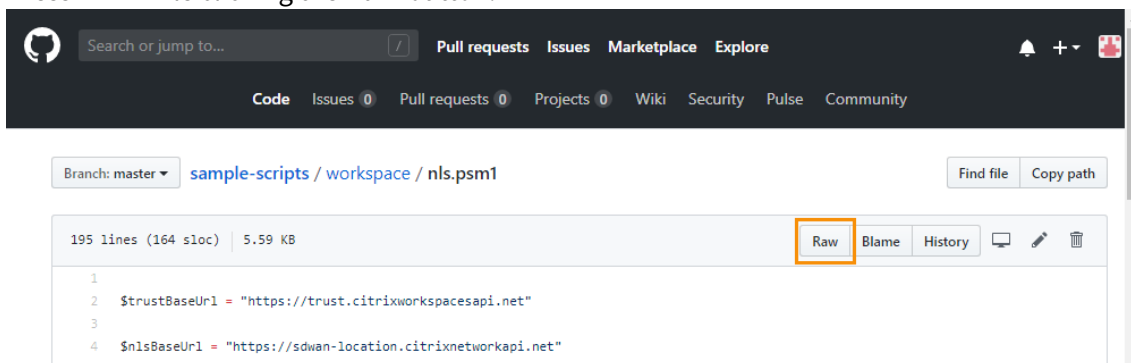
1. Determine the public IP address ranges of each branch location that your internal users connect from.
2. Download the PowerShell module.
3. Create a secure API client in Citrix Cloud and make a note of the Client ID and secret.
4. Import the PowerShell module and connect to the Network Location Service (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.

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/nls.psm1>.
2. Press **ALT** while clicking the **Raw** button.



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

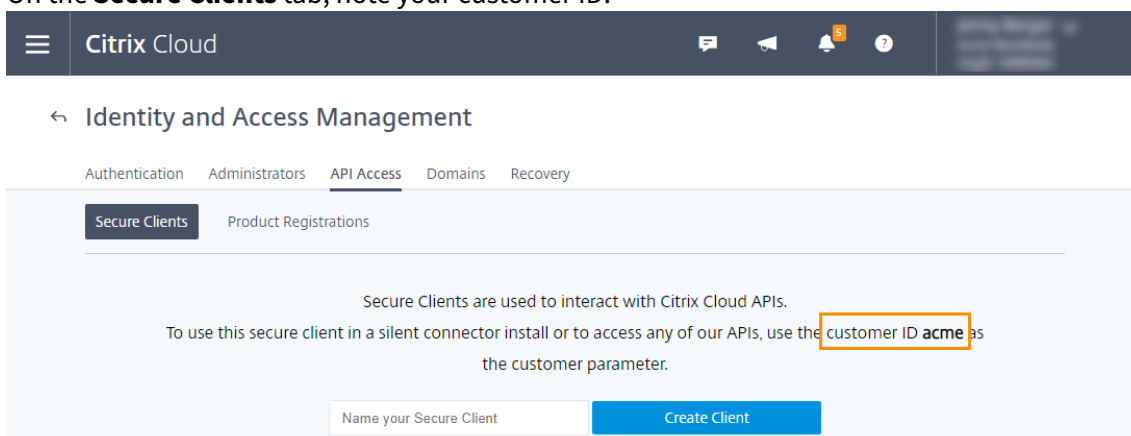
Required configuration details

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 will be 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.



- X



Copy



Copy

Close

Download

- `$clientId` = "YourSecureClientID"
- `$customer` = "YourCustomerID"
- `$clientSecret` = "YourSecureClientSecret"

- ```
1 Connect-NLS -clientId $clientId -clientSecret $clientSecret -
```

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

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

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

**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 appropriate values for each parameter, one at a time. When entering values for the `-tags` parameter, press ENTER after entering each tag value. When you're finished entering tags, press ENTER again to proceed to the next parameter.

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 will be 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.

**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 Virtual Apps and Desktops console.
- Use ICA file logging to verify the correct addressing of the client connection.

**Virtual Apps and Desktops service 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.

**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.

For direct VDA connections, the **Address** property contains the VDA's IP address and port and the **SSL-ProxyHost** property contains the VDA's FQDN and port.

For gateway connections, the **Address** property contains the STA ticket and the **SSLProxyHost** property contains the gateway's FQDN and port.

## 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] -ipv4Ranges @"1.2.3.4/32","4.3.2.1/32" | Set-NLSSite
```

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] -ipv4Ranges @"98.0.0.1/32","141.43.0.0/24" | Set-NLSSite
```

## 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`.

## 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.

```
1 Import-Module .\nls.psm1 -Force
2
3 $clientId = "XXXX" #Replace with your clientId
4 $clientSecret = "YYY" #Replace with your clientSecret
```

```
5 $customer = "CCCCC" #Replace with your customerid
6
7 # Connect to Network Location Service
8 Connect-NLS -clientId $clientId -clientSecret $clientSecret -customer
 $customer
9
10 # Create a new Network Location Service Site (Replace with details
 corresponding to your branch locations)
11 New-NLSSite -name "New York" -tags @("EastCoast") -ipv4Ranges @("
 1.2.3.0/24") -longitude 40.7128 -latitude -74.0060
12
13 # Get the existing Network Location Service Sites (optional)
14 Get-NLSSite
15
16 # Update the IP Address ranges of your first Network Location Service
 Site (optional)
17 $s = (Get-NLSSite)[0]
18 $s.ipv4Ranges = @("1.2.3.4/32","4.3.2.1/32")
19 $s | Set-NLSSite
20
21 # Remove all Network Location Service Sites (optional)
22 Get-NLSSite | Remove-NLSSite
23
24 # Remove your third site (optional)
25 (Get-NLSSite)[2] | Remove-NLSSite
```

## Troubleshooting

### VDA launch failures

If VDA sessions are failing to launch, verify you are 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. For more information, see Requirements in this article.

To verify a VDA's public IP address, log on to each VDA machine, visit <https://google.com>, and enter "what is my ip" in the search bar.

### 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 are using the correct IP address ranges for the networks where your internal users are connecting from. These are generally the public IP address ranges that correspond to the networks



where your VDAs reside, although your users might access the VDAs through a VPN. Do not use the local IP addresses of the VDAs. For more information, see Requirements in this article.

To verify a VDA's public IP address, log on to each VDA machine, visit <https://google.com>, and enter "what is my ip" in the search bar.

### **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](#).

## **Secure workspaces**

July 13, 2021

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

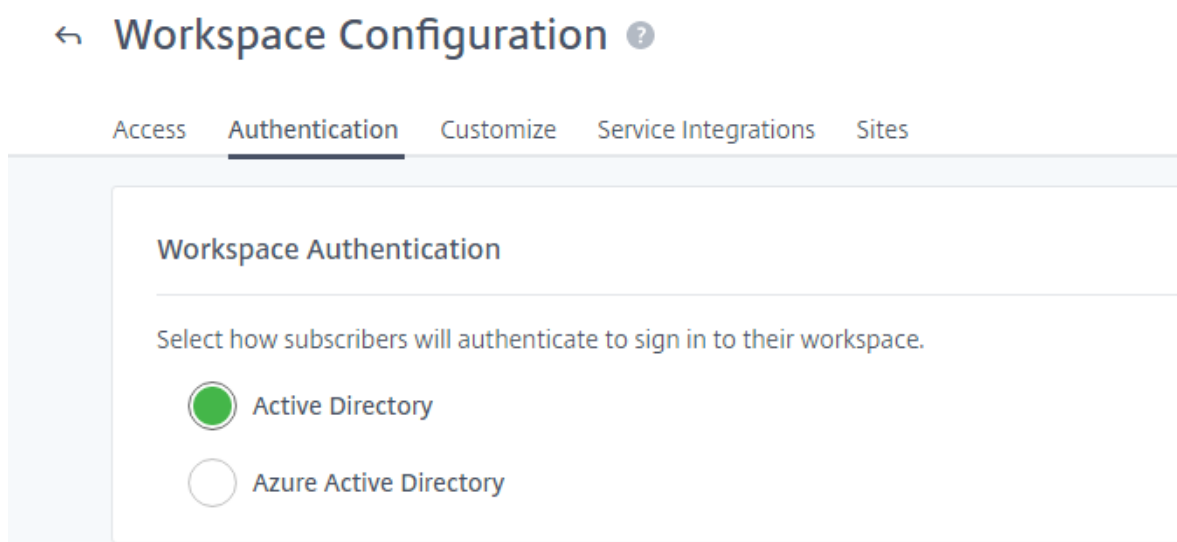
- Active Directory
- Active Directory plus token
- Azure Active Directory
- Citrix Gateway
- Okta
- SAML 2.0

These authentication options are available to any Citrix Cloud service.

Citrix Workspace also supports using Citrix Federated Authentication Service (FAS) to provide single sign-on to virtual apps and desktops.

## Change authentication methods

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 the authentication methods to periods of low usage. If you do have subscribers logged on to Citrix Workspace using a browser or Citrix Workspace app, please advise them to close the browser or exit the app. After waiting approximately five minutes, they can log back on again using the new authentication method.

## Active Directory

By default, Citrix Cloud uses Active Directory to manage subscriber authentication to workspaces. Using Active Directory requires that you have at least two Citrix Cloud Connectors installed in the on-premises Active Directory domain. For more information about installing the Cloud Connector, see [Cloud Connector Installation](#).

## Active Directory plus token

For additional security, Citrix Workspace supports a token as a second factor of authentication in addition to Active Directory sign-in.

When you use Active Directory plus token authentication, Workspace prompts all subscribers during every sign-in to enter a token from their enrolled device. Subscribers can enroll their devices by following the steps in [Register devices for two-factor authentication](#). Currently, subscribers can enroll

only one device at a time.

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](#).
- In the Citrix Cloud console, **Active Directory + Token** authentication enabled on the **Identity and Access Management** page. For more information, see [To enable Active Directory plus token authentication](#).
- Subscribers need access to email to enroll devices.
- 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.

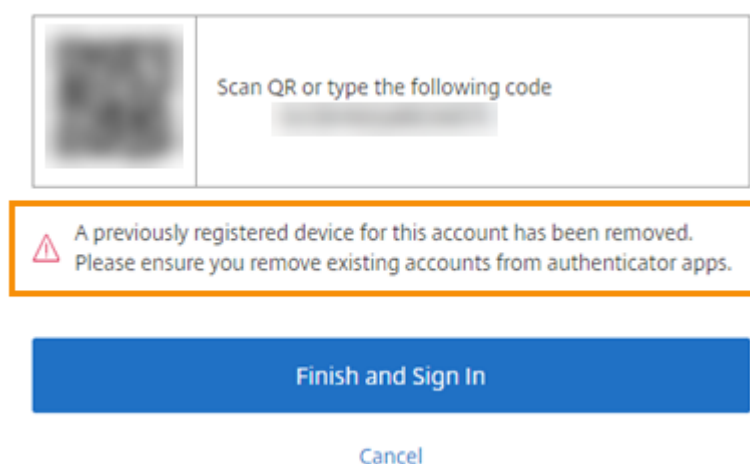
### Important:

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 Workspace with two-factor authentication is not supported. Only verification codes that are generated from an authentication app on an enrolled device are supported tokens for two-factor authentication.

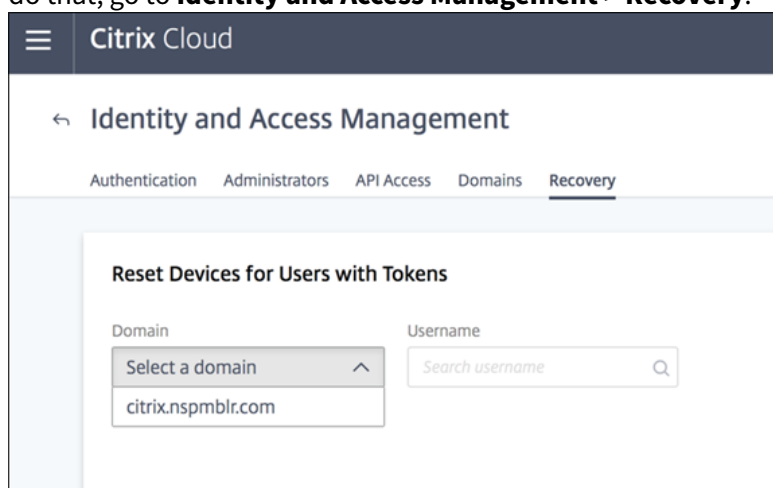
### To re-enroll devices

If a subscriber no longer has their enrolled device or needs to re-enroll it (for example, after erasing all 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 described in [Register devices for two-factor authentication](#).

## 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 about 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 Active Directory 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 are not synchronized, certain workflows in Citrix Workspace will fail.

### Warning:

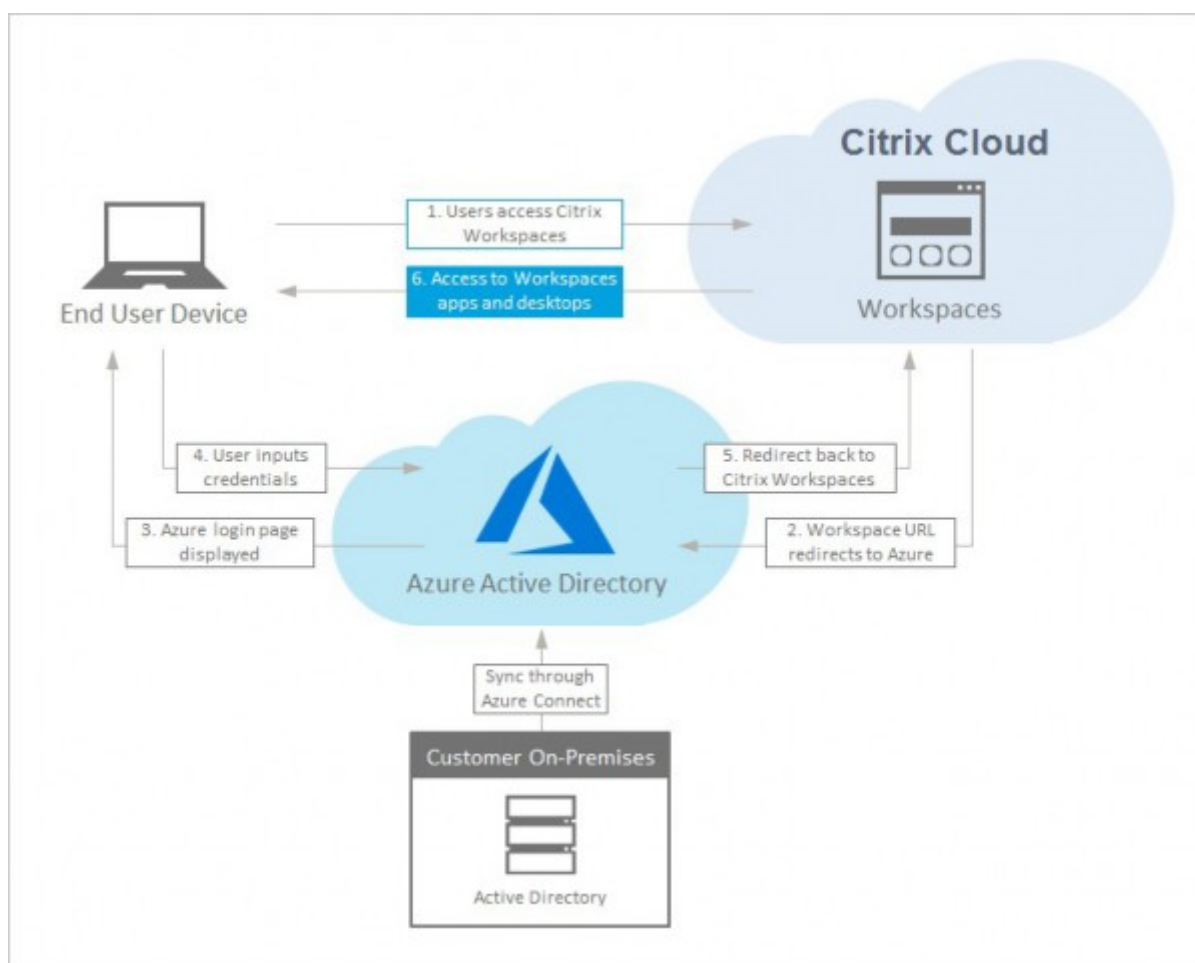
- If you are using Azure AD, do not make the registry change described in [CTX225819](#). Making this change may cause session launch failures for Azure AD users.
- Adding a group as a member of another group (nesting) is not supported for federated authentication using Azure AD. If you do assign a nested group to a catalog, members of that group can't access apps from the catalog.

After enabling Azure AD authentication:

- **Manage users and user groups by using Citrix Cloud Library:** Use only the Citrix Cloud Library to manage users and user groups. (Do not specify users and user groups when creating or editing Delivery Groups.)
- **Added security:** Users are prompted to sign in again when launching an app or a desktop. This is intentional and provides more security, because the password information flows directly from user's device to the VDA that is hosting the session.
- **Sign-in experience:** Users have a different sign-in experience in Azure AD. Selecting Azure AD authentication provides federated sign-in, not single sign-on. Users sign in to workspace from an Azure sign-in page, however they may have to authenticate a second time when opening an app or desktop from the Citrix Virtual Apps and Desktops service. To achieve single sign-on and prevent a second logon prompt, you need to 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.

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 are performing federation, your AD users must be synchronized to the federation provider. Citrix Cloud requires the AD attributes to allow your 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 is enabled on the **Identity and Access Management** page. This action 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 with 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 (for example, RADIUS MFA, smart card, 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.

### **Okta**

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

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 need to 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 on the **Identity and Access Management** page.

For more information, see [Connect Okta as an identity provider to Citrix Cloud](#).

After enabling Okta authentication, subscribers have a different sign-in experience. Selecting Okta authentication provides federated sign-in, not single sign-on. Subscribers sign in to workspace from an Okta sign-in page, but they may have to authenticate a second time when opening an app or desktop from the Citrix Virtual Apps and Desktops service. To enable single sign-on and prevent a second logon prompt, you need to use the Citrix Federated Authentication Service with Citrix Cloud. See [Enable single sign-on for workspaces with Citrix Federated Authentication Service](#) for more information.

### **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.

**Note:**

Enabling Okta authentication provides federated sign-in, not single sign-on. Subscribers sign in to workspaces from an Okta sign-in page, but they may have to authenticate a second time when opening an app or desktop from the Citrix Virtual Apps and Desktops service. To enable single sign-on and prevent a second logon prompt, you need to use the Citrix Federated Authentication Service with 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.

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 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**

Citrix Workspace supports using Citrix Federated Authentication Service (FAS) to provide single sign-on to virtual apps and desktops. Subscribers signing in to their workspaces through Azure AD enter



their credentials only once to access their 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. This connection is created through the **Connect to Citrix Cloud** option in the FAS installer. 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 where you want your FAS server to reside. Single sign-on is active for subscribers only in the resource locations where FAS servers are present.
- A connection between your on-premises Active Directory domain and Citrix Cloud, with FAS enabled in Workspace Configuration.

For more information about using FAS with Citrix Cloud, see [Enable single sign-on for workspaces with Citrix Federated Authentication Service](#).

### Subscriber sign-out experience

#### Important:

If Citrix Workspace times out in the browser due to inactivity, subscribers remain signed in to Azure AD. This is by design, to prevent a Citrix Workspace time out from forcing other Azure AD applications to close.

To close Citrix Workspace, use **Settings > Log Off**. That option completes the sign-out process from the workspace and Azure AD. If subscribers close the browser instead of using the **Log Off** option, they might remain signed in to Azure AD.

## Service continuity

October 1, 2021

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

Service continuity allows users to connect to their virtual apps and desktops during outages, as long as the user device maintains a network connection to a resource location. Users can connect to virtual 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 Virtual Apps and Desktops 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.

## User experience during an outage

When service continuity is enabled, the user experience during an outage varies depending on:

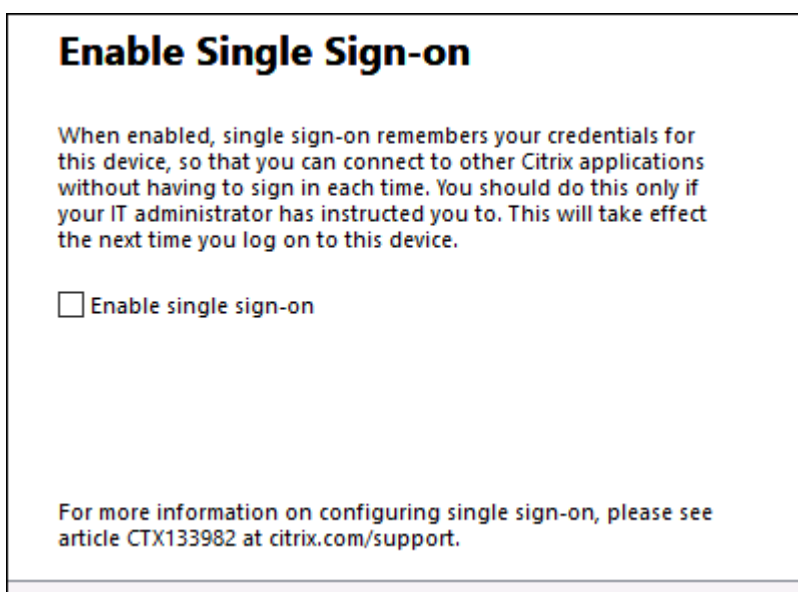
- The type of outage
- Whether the Citrix Workspace app is configured with domain pass-through authentication
- Whether session sharing is enabled for the app or desktop the user connects to

For some outages, users continue accessing their virtual apps and desktops with no change to their user experience.

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.

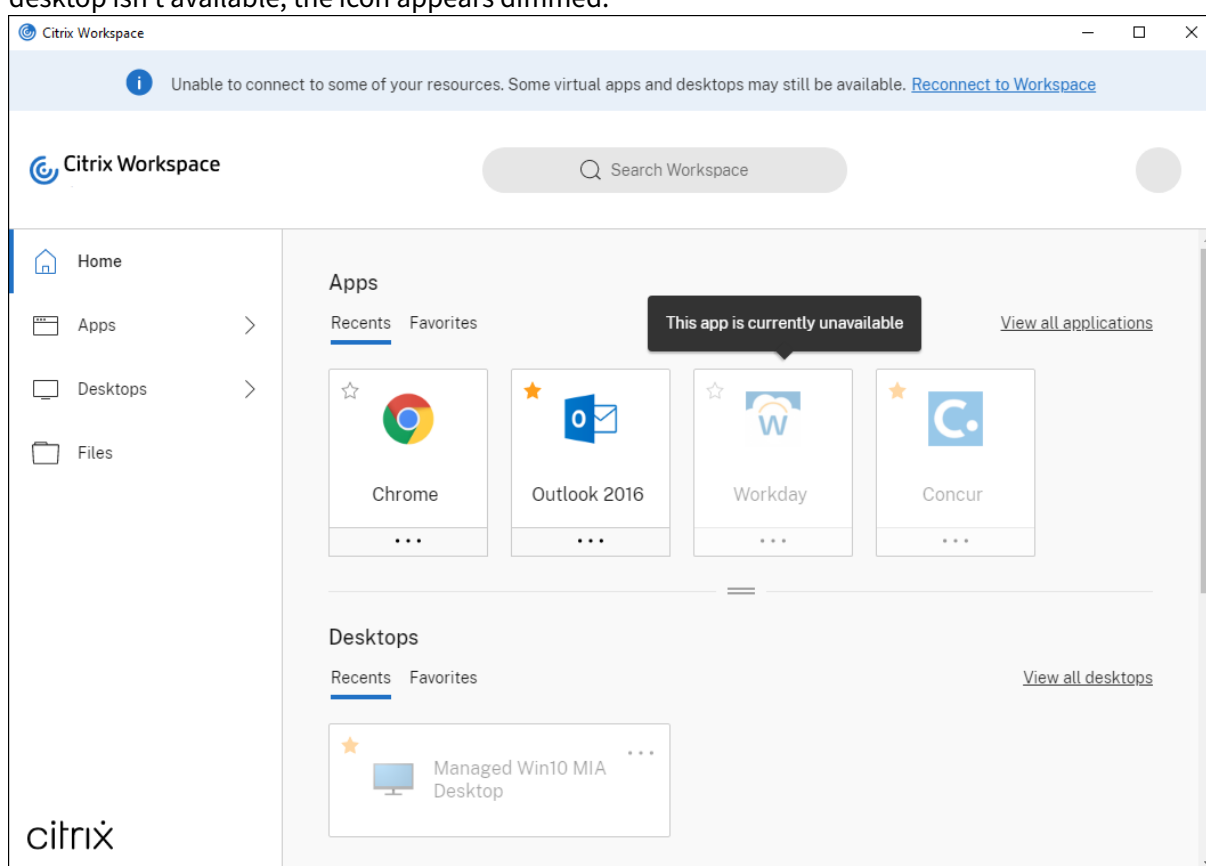
### Note

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](#).

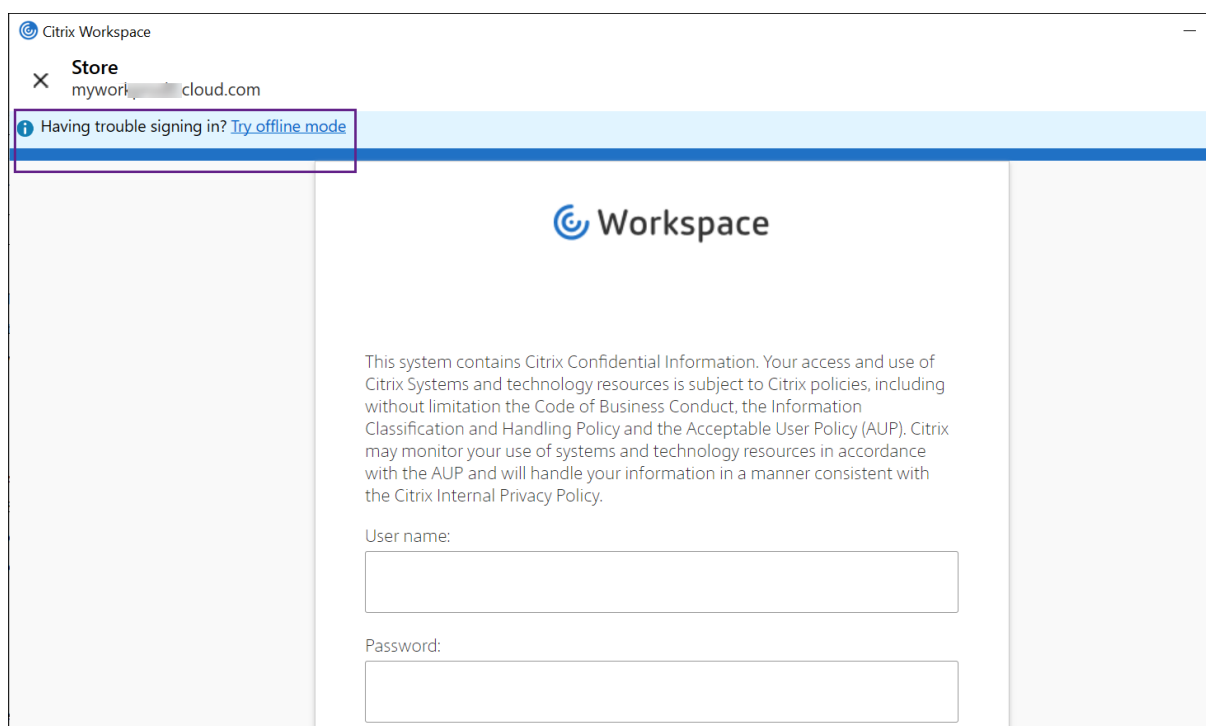
In all other configurations, users are prompted to reenter their AD credentials at the VDA before accessing resources.

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 30 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](#).

## Requirements and limitations

### Site requirements

- Supported in all editions of the Citrix Virtual Apps and Desktops service and Citrix Virtual Apps and Desktops Standard for Azure, when using Workspace Experience.
- Not supported for Citrix Workspace with site aggregation to on-premises Virtual Apps and Desktops.
- Not supported for on-premises Citrix Gateway.

### User requirements

- Citrix Workspace app 2106 for Windows, Citrix Workspace app 2106 for Mac, or Citrix Workspace app 2106 for Linux at a minimum.

### 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:

- Citrix Workspace app 2109 for Windows
- Google Chrome and Microsoft Edge

See Service continuity in browser.

- Supported for the Citrix Workspace app in native app only. Not supported for Citrix Workspace app for Web.
- 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 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](#).

## 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

### Note:

If you're using Citrix Hypervisor or vSphere with Autoscale, then power management is available even during Cloud Delivery Controller outages.

- 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.

For more information about available VDA functions during outages, see VDA management during outages.

## App protection limitations

If app protection policies are enabled for an app or desktop, the icon for that app or desktop doesn't appear in the Citrix Workspace home page during outages. Users can't access these resources during outages.

For more information about app protection policies, see [App protection](#).

## Unicode and ASCII user name requirements and limitations

Service continuity might not support all users who have Unicode user names on their Windows devices but ASCII user names for their Citrix Workspace account. If the Unicode user name contains Cyrillic or eastern Asian characters, Workspace connection leases fail to launch for these users.

## 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 outside or inside your LAN.

To 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**.

To 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.



## Optimize connectivity to workspaces

When service continuity is enabled, Direct Workload Connection is not available during outages. (Direct Workload Connection allows internal users to bypass the gateway and connect to VDAs directly, reducing latency for internal network traffic. For more information, see [Optimize connectivity to workspaces with Direct Workload Connection](#).)

If you are publishing apps or desktops from a resource location that is accessible internally and externally, you can reduce latency for internal network traffic. To reduce latency, allow internal users to bypass the gateway and connect directly to the resource location.

Use this PowerShell command:

```
Set-ConfigZone -InputObject (get-configzone -ExternalUid resourceLocation GUID) -EnableHybridConnectivityForResourceLeases $true
```

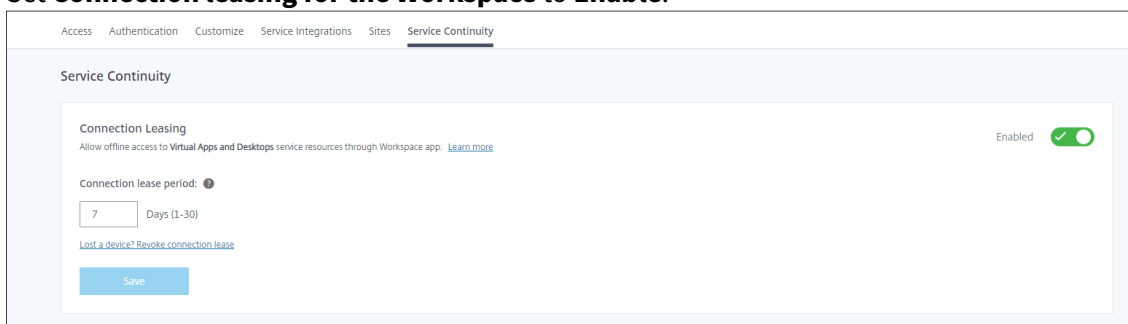
Replace `resourceLocation GUID` with the global unique identifier of the resource location.

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.

## Configure service continuity

To enable service continuity for your site:

1. From the Citrix Cloud menu, go to **Workspace Configuration > Service continuity**.
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.

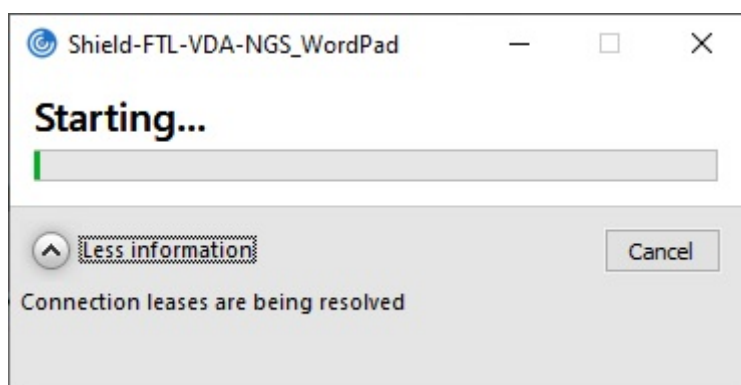
### How sessions launch during outages

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.

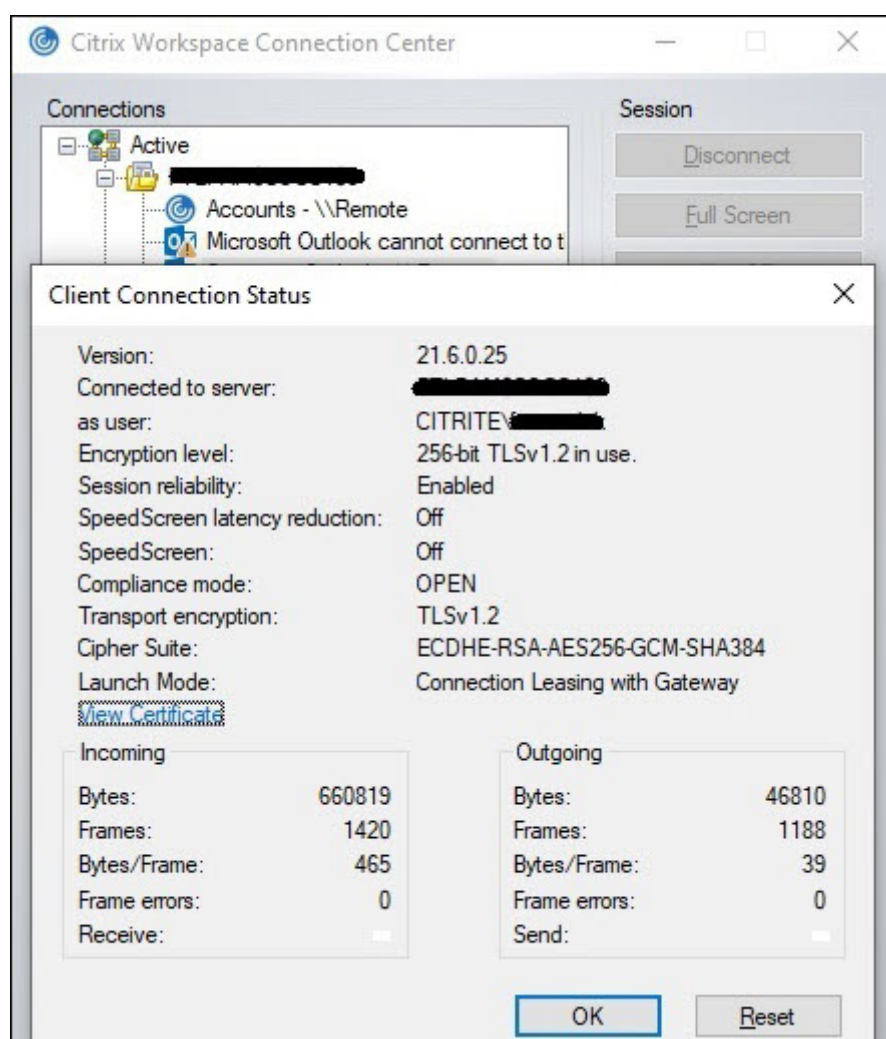
When the Citrix Cloud broker is online, the Cloud Connector uses the Citrix Cloud broker to resolve which VDA is available. When the Citrix Cloud broker is offline, the secondary broker for the Cloud Connector (also known as the High Availability service) listens for and processes connection requests.

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-nnnnnnn
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 to 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 your site uses Citrix Hypervisor or vSphere, Citrix Host Service can provide hypervisor credentials to Cloud Connector. If your site uses any other hypervisor, such as VMs stored in Azure, Citrix Host Service can't provide hypervisor credentials to the Cloud Connector. This means:

- If your site uses Citrix Hypervisor or vSphere: The Cloud Connector can perform power management operations, including the Pooled VDI case, during an outage.
- If your site uses any other hypervisor: 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 **Shutdown-DesktopsAfterUse** property enabled are placed into maintenance mode when an outage in the Citrix-managed broker occurs. You can change this setting to allow those desktops to be used during an outage. However, power management is only available during an outage if you're using Autoscale with Citrix Hypervisor or vSphere. If those desktops are used during an outage, they might contain data from the previous user because they haven't been 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                        |

### **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. Citrix Workspace app 2109 for Windows is 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.

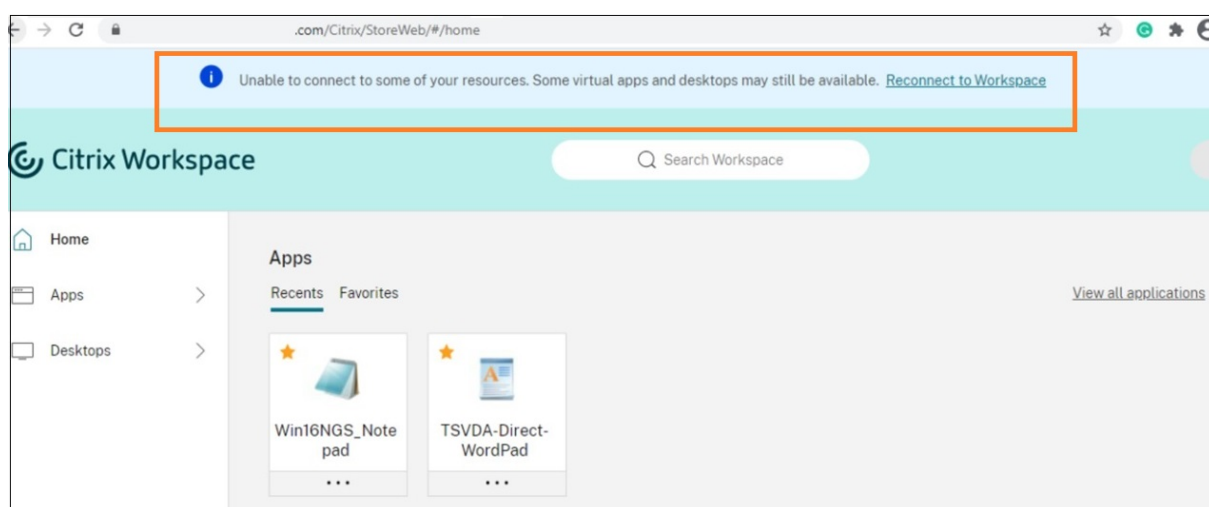
### Browser user experience

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

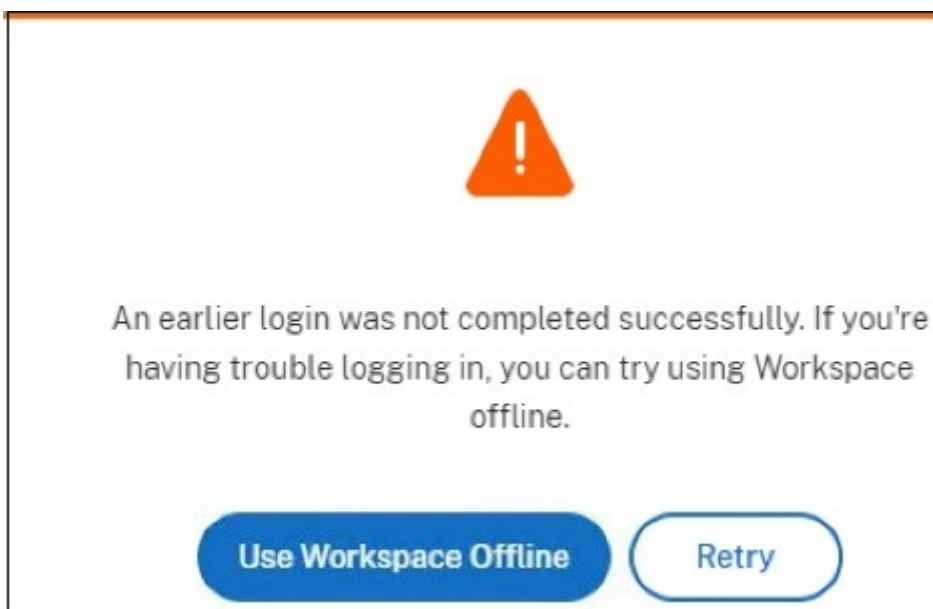
Users can access their apps and desktops from a browser during outages, as long as the user device maintains a network connection to a resource location.

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:



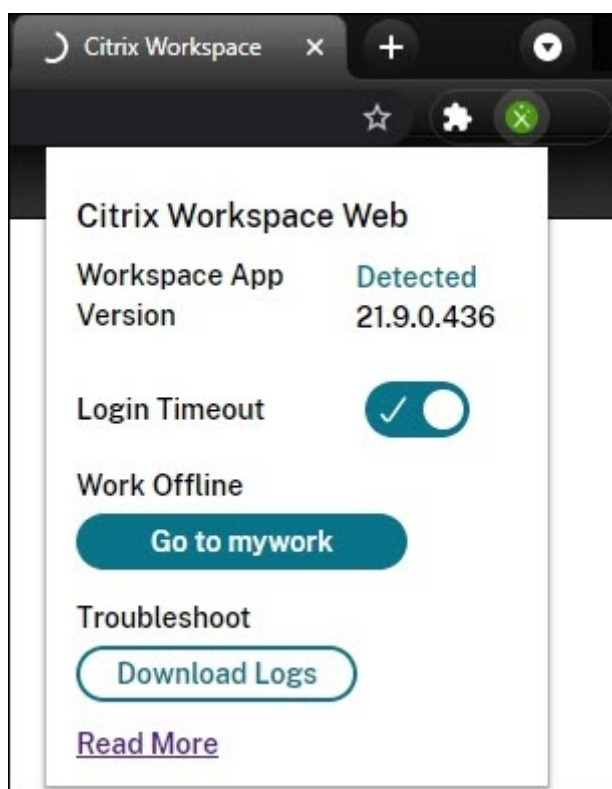
Users can access apps and desktops that are available offline by clicking any icon that is not dimmed. Users can also try to get back online by clicking **Reconnect to Workspace**.

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 appear.

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

Ensure that the extension icon in the browser appears green.

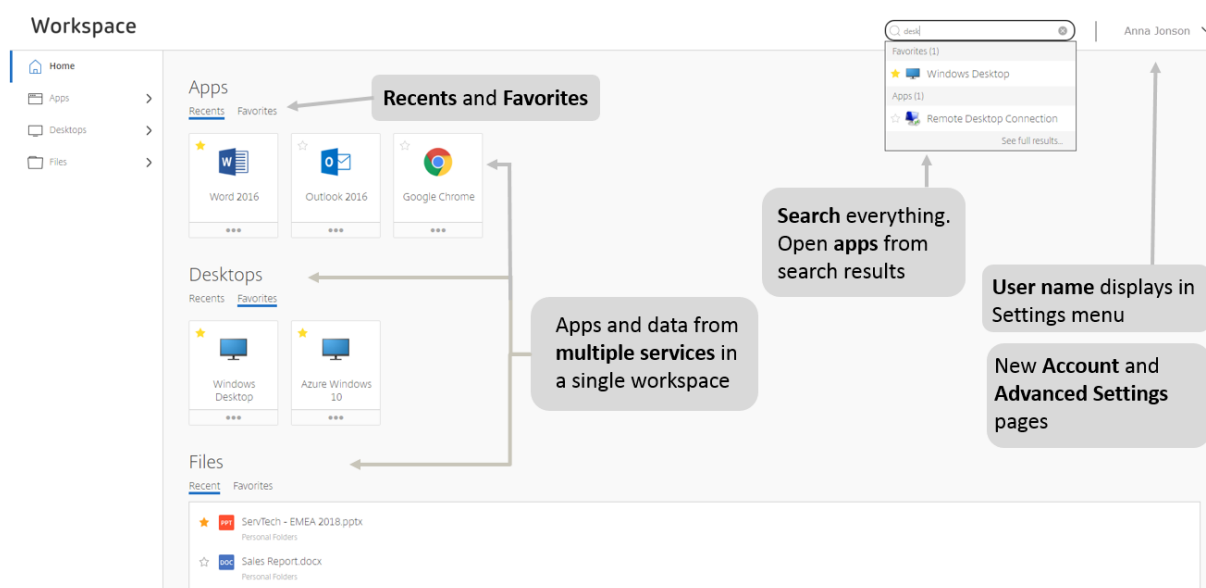
To download logs, click the extension icon in the browser. Then click **Download Logs**.

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 Citrix Workspace App**. If this option is set to **Use Web Browser**, service continuity isn't supported in the browser.

## Manage your workspace experience

March 24, 2021

This article describes what subscribers see after signing in and how they can interact with their workspace, including guidance for common issues.



## Browser support

Access workspaces using Internet Explorer 11, or the latest version of Edge, Chrome, Firefox, or Safari.

## Workspace features

### Card layout

Apps and desktops in your workspace are represented in a “card” layout. A pop-up window shows more details and actions.

### Search

You can search everything in your workspace and open apps directly from the search results. Search requires a minimum of three characters.

### Recents

Recents displays recently opened apps, desktops, and files. For apps and desktops, depending on screen size, you see up to 30 (of each). For files, you see up to 15.

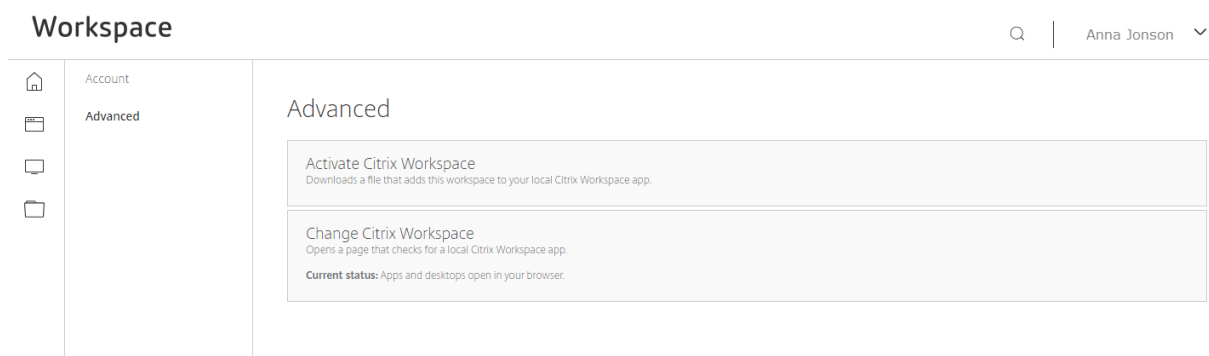
### Favorites

Select the star icon to add an app to Favorites (max 250). Administrators configure this option, so it might not be available.

### Settings

Access settings from the drop-down menu. The menu contains the user name. The user name comes from the Active Directory display name. If the display name is left blank (we do not recommend this), the domain and account name display.

Select **Account Settings** for more options.



- **Activate Citrix Workspace.** Downloads a file that adds this workspace to your local Citrix Workspace app.
- **Change Citrix Workspace.** Opens a page that checks for a local Citrix Workspace app. This option is not available in Internet Explorer 11.

#### Note:

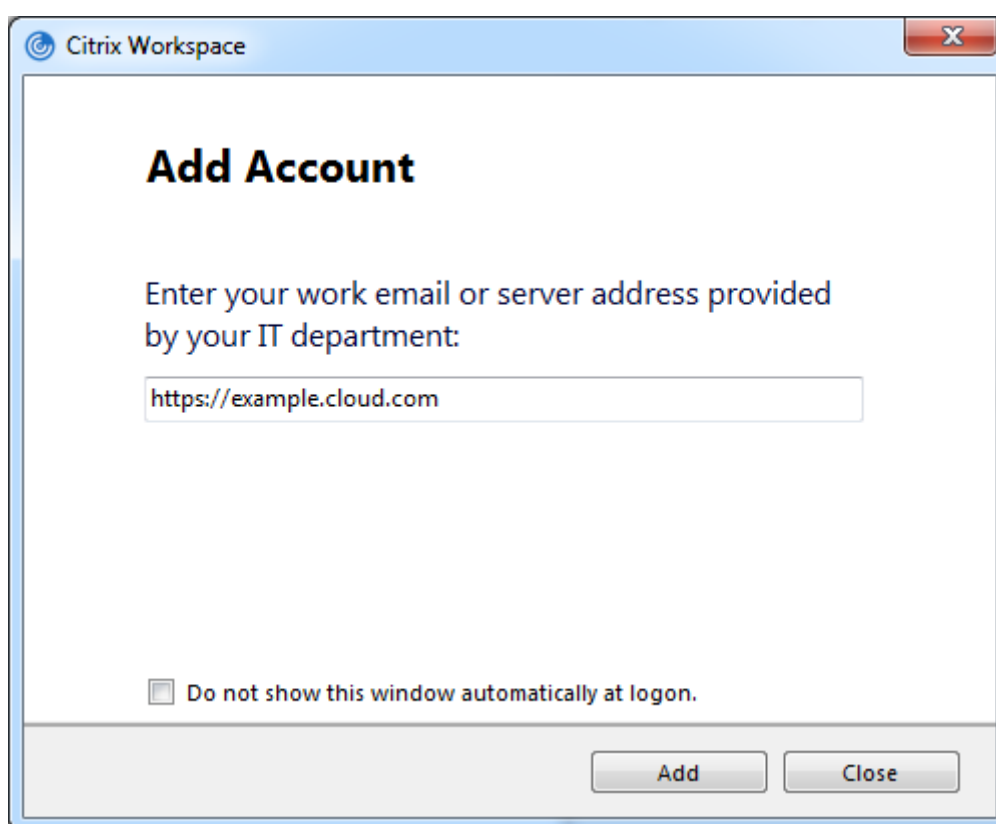
This option is only available with Citrix Virtual Apps and Desktops services. **Change Citrix Workspace** is not available if, for example, you are only using SaaS apps through the Citrix Gateway service.

- **Download Citrix Workspace.** Downloads an installation file to your machine. Run the file to install a local Citrix Workspace app for Windows or Mac.

## Changes to your service subscription

If you have changed your service subscription, you may need to refresh the local Workspace app manually. In Citrix Workspace app for Windows:

1. From the Windows system tray, right-click the Citrix Workspace icon, and select **Advanced Preferences > Reset Citrix Workspace**.
2. Open Citrix Workspace app for Windows, then select **Accounts > Add**, and enter the workspace address, for example, <https://example.cloud.com>.



As an alternative to step 2, you can use a browser to enter the workspace URL and sign in. Then, activate Citrix Workspace from **Settings > Account Settings > Activate Citrix Workspace**. Activating Citrix Workspace downloads a file with a .CR extension that adds the workspace to your local Citrix Workspace app.

## Errors from authentication changes

Subscribers who are logged on to Citrix Workspace may see errors if an administrator changes the authentication method, for example, from Active Directory to Azure Active Directory. If this happens, log

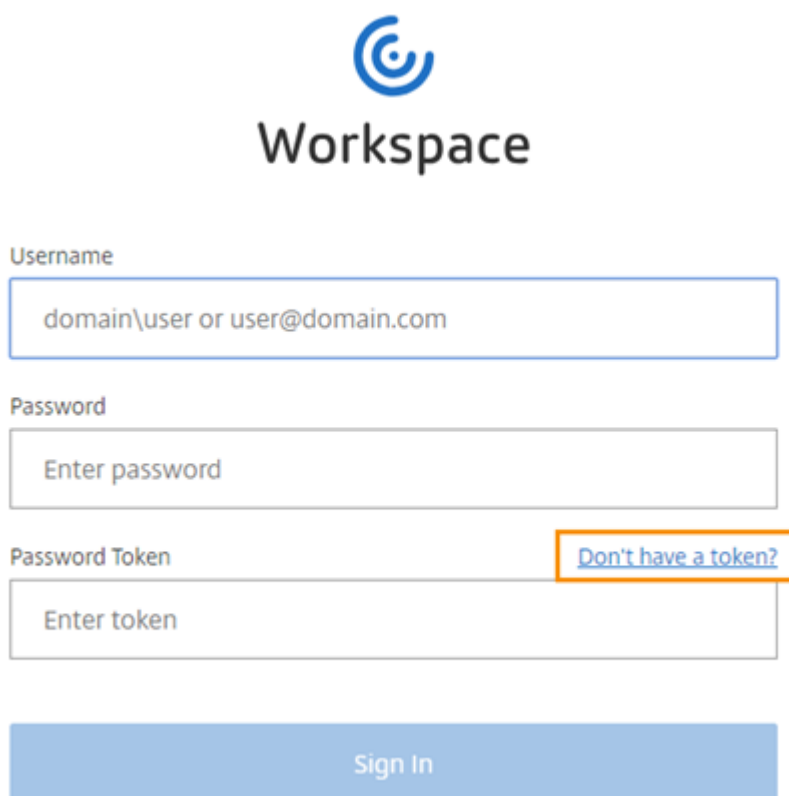


off Citrix Workspace and close the browser or Citrix Workspace app. Wait approximately 5 minutes and log back on. When Citrix Workspace is available again, you can log on using the new authentication method.

### Register devices for two-factor authentication

Before subscribers can use two-factor authentication plus token with Workspace, they must register their device. During registration, Workspace presents a QR code for the subscriber to scan with an app that follows the [Time-Based One-Time Password](#) standard, such as Citrix SSO. For a smooth registration process, Citrix recommends downloading and installing this app on the device beforehand.

1. From a computer, open a browser, navigate to the Workspace sign-in page, and select **Don't have a token?**



Username

domain\user or user@domain.com

Password

Enter password

Password Token

Enter token

[Don't have a token?](#)

Sign In

2. Enter your user name in domain\username format or your company email address and select **Next**.



To register a token device, you first need to verify your identity. Enter your username below to send an email with a verification code.

Username

Next

[Cancel](#)

Citrix Cloud sends you an email with a verification code. This verification code is temporary and is only used to register your device. Do not use this temporary code to sign in to Workspace with two-factor authentication.



Hello 

To complete registration of your token device, enter the following verification code:

Verification code:

**405239**

Your code is valid for 24 hours and can only be used once.

3. After you receive the email, enter the verification code and your Active Directory account password when prompted. Select **Next**.

Enter your verification code and password below to continue registering your token device. Didn't receive a code? [Resend verification email](#).

Verification Code

Password

[Next](#)

[Cancel](#)

- From the authenticator app, scan the QR code or enter the verification code manually.



- Select **Finish and Sign In** to complete the registration.

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

The diagram shows the sign-in process. On the left is a screenshot of the Citrix SSO app with the 'Password Tokens' tab selected. A box highlights the token '569270' under 'My Device'. An arrow points from this token to the 'Enter token' field on the Workspace sign-in page. The Workspace sign-in page includes fields for 'Username' (with a hint 'domain\user or user@domain.com'), 'Password' (with a hint 'Enter password'), and 'Password Token' (with a hint 'Enter token'). There is also a 'Don't have a token?' link and a 'Sign In' button.

### Important:

Obtaining temporary email-based tokens is not a supported method for signing in when two-

factor authentication is enabled for Workspace. To sign in with two-factor authentication, subscribers must register a device with an authenticator app installed. Subscribers must not use the temporary email token sent during the registration process. Only verification codes that are generated from an authentication app on an enrolled device are supported tokens for two-factor authentication.

## Notifications in Workspace

September 2, 2021

### Search notifications

**Note:**

Activity feed search is available in Workspace on Web and Desktop in US and EU accounts.

Activity feed search is offered as a public tech preview and is not currently HIPAA compliant.

Workspace users can search their activity feed and filter the results to find microapp notifications and integrations quickly. Users can also action notifications directly from their search results.

Click the search box at the top of the Workspace UI to bring up a Quick Search Box to enter a query. After entering a query, press Enter, or select **See more results**.




Select **Feed** in the top menu to see all matching results. You can also filter results by **Status**, **Source**, **Action required**, and **Time period**.

Search results for 'Citrix'

AllApplicationsDesktopsFilesFeed

Feed




Citrix TIPS: Scoring an A+ with HTTP headers and Citrix Gateway

Active

14 hours ago

Citrix Blogs




Transition to a resilient, secure hybrid work model with Citrix and Google

Active

7 hours ago

Citrix Blogs




New Course Available

Active

The eCWS-2024: Introduction to Citrix Secure Internet Access for Citrix Virtual Apps and Desktops Course has been released.

23 days ago

Citrix Education



New Course Available

Active

The eCNS-2024: Deploy Citrix SD-WAN through SD-WAN Orchestrator Course has been released

Filters

Status

Dismissed0

Active4

Source

Citrix Blogs2

Citrix Education2


Action Required

Show only items that require action

Time Period

Past year (4)

Select any search result to open your notification feed to see more information and complete any available actions:



Blog Post details

Citrix Blogs • 14 hours ago

X

Written by Michael McAlpine - Published at 2021-08-31 12:00:08.0

HTTP security headers are a fundamental part of securing a web site. They help to enhance the overall security of a web application by preventing the exploitation of potential vulnerabilities. The goal of improving HTTP headers is to prevent an ...

The post [Citrix TIPS: Scoring an A+ with HTTP headers and Citrix Gateway](#) first appeared on [Citrix Blogs](#).

Like

Related Stories

Boost your performance with Citrix ADC

Citrix TIPS: Moving off deprecated Citrix ADC features for Citrix Gateway

The Citrix SD-WAN and Microsoft Azure Virtual WAN advantage

View Blog Post

© 1999–2021 Citrix Systems, Inc. All rights reserved.

118

## Fall back to StoreFront

September 30, 2021

**Fall back to StoreFront** is a resiliency feature that provides temporary access to Citrix Virtual Apps and Desktops through your StoreFront instance during a Workspace outage. You can use any valid URL to access Citrix Virtual Apps and Desktops, but Citrix recommends that you use one of the following to fall back to StoreFront:

- A single internal URL or list of URLs that resolve to StoreFront servers inside your corporate network.
- A single external URL or list of external URLs that resolve to Citrix Gateway with StoreFront deployed behind it.
- A GSLB URL, which resolves to a GSLB layer of multiple Citrix Gateways with StoreFront behind them.

The **Fall back to StoreFront** feature is configured using PowerShell, which performs authenticated REST API calls to your Citrix Cloud customer. The PowerShell cmdlets are provided within a standalone PowerShell module, which can be downloaded and run from any computer with internet access.

**Note:**

The downloaded PowerShell module is a different SDK from the RemotePowerShell SDK that is used to configure the Citrix Virtual Apps and Desktops service.

### Configure fall back to StoreFront

Fall back to StoreFront configuration with PowerShell involves the following tasks:

1. Download the PowerShell module.
2. Create and store a Citrix Cloud API client and secret.
3. Identify the URLs of your GSLB, Gateway, or StoreFront instances.
4. Import the PowerShell module and configure one or more StoreFront fall back URLs.
5. Verify that your StoreFront fall back URL has been configured correctly.

### Download the PowerShell module

Before you configure **Fall back to StoreFront**, download and unpack the Citrix-provided [PowerShell module](#) from GitHub. The file includes `Citrix.Workspace.FallbackConfiguration.psm1` and `Citrix.Workspace.FallbackConfiguration.psd1`

**Important:**

The PowerShell script provided is designed for customers in the EU, US, and AP-S regions. Citrix Cloud customers in the Japan region must use a .json configuration file to target the REST API calls to Citrix Cloud for Japan. If your customer is in Citrix Cloud Commercial EU, US, and AP-S, you can ignore this step and remove references to the `$env:CTXSWSPSHSETTINGS` variable from the script.

Citrix Cloud customers in the Japan region must also download the [jp-production.json](#).

**Required configuration details**

To configure **Fall back to StoreFront**, you need the following:

- The URLs of your GSLB, Gateway, or StoreFront instances.
- A Citrix Cloud API client and secret.

If you don't already have a Citrix Cloud API client and secret, you can create one by following this article: <https://developer.cloud.com/explore-more-apis-and-sdk/cloud-services-platform/citrix-cloud-api-overview/docs/get-started-with-citrix-cloud-apis>. Store these credentials safely and treat them as sensitive data.

**Configure StoreFront fall back URLs**

1. Unzip the FallbackPowershellModule.zip file to a suitable directory from where you want to run the PowerShell, such as your current user's desktop.
2. Open the PowerShell ISE and select **New\*** in the **File** menu.
3. Copy the example script into the interactive PowerShell window so that you can modify and run it against your own **Citrix Cloud** customer.
4. Set the `$STFFallbackPath` variable to the path of the directory that you unzipped the FallbackPowershellModule.zip file into.
5. Configure the `$YourCustomerAPIKey`, `$YourCustomerSecretKey`, and `$YourCustomerURL` variables in your PowerShell script with the information that you prepared in the **Required configuration details** step.

```
1 $YourCustomerAPIKey = " "
2 $YourCustomerSecretKey = " "
3 $YourCustomerURL = "https://<yourcustomer>.cloud.com"
4 <!--NeedCopy-->
```

6. Import the PowerShell module



```

1 if(Test-Path -Path "$STFFallbackPath\Citrix.Workspace.
 FallbackConfiguration.psm1")
2 {
3
4 Write-Host "Importing STF Fallback Powershell Module..." -
 ForegroundColor "Green"
5 Import-Module -Name "$STFFallbackPath\Citrix.Workspace.
 FallbackConfiguration.psm1" -verbose
6 }
7
8 else
9 {
10
11 Write-Host "STF Fallback Powershell Module not found inside
 $STFFallbackPath" -ForegroundColor "Red"
12 }
13
14 <!--NeedCopy-->

```

7. Configure one or more StoreFront fall back URLs by updating the `ServiceTitle` and `StoreWebAddress` parameters. `ServiceTitle` is the meaningful name you want your subscribers to see such as "StoreFront EU". `StoreWebAddress` is the full path to Receiver for Web or a Gateway URL. The following example includes three StoreFront fall back URLs:

```

1 Set-WorkspaceFallbackConfiguration -WorkspaceUrl $YourCustomerURL
 `
2 -ClientId $YourCustomerAPIKey `
3 -ClientSecret
 $YourCustomerSecretKey `
4 -Configuration @{
5 "ServiceTitle" = "StoreFront EU"; "StoreWebAddress" = "https://
 storefront-eu.example.com/Citrix/StoreWeb/" }
6 , `
7 @{
8 "ServiceTitle" = "StoreFront US"; "StoreWebAddress" = "https://
 storefront-us.domain.com/Citrix/StoreWeb/" }
9 , `
10 @{
11 "ServiceTitle" = "StoreFront APAC"; "StoreWebAddress" = "https
 ://storefront-apac.domain.com/Citrix/StoreWeb/" }
12
13 <!--NeedCopy-->

```

8. To verify that your StoreFront fall back URL has been configured correctly, follow the instruc-

tions under **View StoreFront fall back URLs**.

### View StoreFront fall back URLs

To see the StoreFront fall back URLs that you've configured, run the `Get-WorkspaceFallbackConfiguration` cmdlet.

```
1 Get-WorkspaceFallbackConfiguration -WorkspaceUrl $YourCustomerURL `
2 -ClientId $YourCustomerAPIKey `
3 -ClientSecret $YourCustomerAPIKey `
4 -Verbose
5 <!--NeedCopy-->
```

### Remove StoreFront fall back URLs

To remove the StoreFront fall back URLs that you've configured, run the `Remove-WorkspaceFallbackConfiguration` cmdlet. All URLs are removed when you use this cmdlet.

```
1 Remove-WorkspaceFallbackConfiguration -WorkspaceUrl $YourCustomerURL `
2 -ClientId $YourCustomerAPIKey `
3 -ClientSecret
4 $YourCustomerSecretKey `
5 -Verbose
6 <!--NeedCopy-->
```

### Example script

The example script includes commands that you might need for adding, viewing, and removing the StoreFront fall back URLs. You don't need to run all commands to perform any single function. For the script to run, always include lines 1–27. If your Citrix Cloud customer is in Japan, also uncomment and run lines 29–43. Afterward, you can include only the commands for the functions you want to perform.

```
1 [Net.ServicePointManager]::SecurityProtocol = [Net.SecurityProtocolType
2]::Tls12
3 [System.Net.ServicePointManager]::SecurityProtocol = [System.Net.
4 SecurityProtocolType]::Tls12;
5 # Your credentials from Citrix Cloud Identity and Access Management
6 [string]$YourCustomerAPIKey = " "
7 [string]$YourCustomerSecretKey = " "
```

```
8 # Commercial US, EU or AP-S
9 [string]$YourCustomerURL = "https://<yourcustomer>.cloud.com"
10
11 # OR
12 # JP region
13 # [string]$YourCustomerURL = "https://<yourcustomer>.citrixcloud.jp"
14
15 # Unpack the .ZIP file containing the PowerShell module to a folder
16 # Point Import-Module to the same path where the Citrix.Workspace.
 FallbackConfiguration.psm1 file is
17 $STFFallbackPath = "$Env:UserProfile\Desktop\Fallback"
18
19 if(Test-Path -Path "$STFFallbackPath\Citrix.Workspace.
 FallbackConfiguration.psm1")
20 {
21
22 Write-Host "Importing STF Fallback Powershell Module..." -
 ForegroundColor "Green"
23 Import-Module -Name "$STFFallbackPath\Citrix.Workspace.
 FallbackConfiguration.psm1" -verbose
24 }
25
26 else
27 {
28
29 Write-Host "STF Fallback Powershell Module not found inside
 $STFFallbackPath" -ForegroundColor "Red"
30 }
31
32
33 <# Uncomment lines 29 - 43 if your Citrix Cloud customer is in Japan
34
35 # Uses jp-production.json file to configure the $env:CTXSWSPOSHSETTINGS
 variable
36 $EnvironmentConfigFile = "jp-production.json"
37 if(Test-Path -Path "$STFFallbackPath\$EnvironmentConfigFile")
38 {
39
40 Write-Host "Setting STF Fallback Environment Variables using
 $EnvironmentConfigFile..." -ForegroundColor "Green"
41 $env:CTXSWSPOSHSETTINGS = "$STFFallbackPath\$EnvironmentConfigFile"
42 }
43
44 else
45 {
```

```
46
47 Write-Host "Path to $EnvironmentConfigFile config file not found."
48 -ForegroundColor "Red"
49 }
50
51 #>
52
53 # Display detailed PowerShell help for the Fallback cmdlets
54 Get-Help Get-WorkspaceFallbackConfiguration -full
55 Get-Help Set-WorkspaceFallbackConfiguration -full
56 Get-Help Remove-WorkspaceFallbackConfiguration -full
57
58 # Perform Fallback admin tasks
59 # Get your existing configuration
60 Get-WorkspaceFallbackConfiguration -WorkspaceUrl $YourCustomerURL `
61 -ClientId $YourCustomerAPIKey `
62 -ClientSecret $YourCustomerAPIKey `
63 -Verbose
64
65 # Add a new or overwrite/update the existing fallback config
66 Set-WorkspaceFallbackConfiguration -WorkspaceUrl $YourCustomerURL `
67 -ClientId $YourCustomerAPIKey `
68 -ClientSecret $YourCustomerSecretKey `
69 -Configuration @{
70 "ServiceTitle" = "StoreFront EU"; "StoreWebAddress" = "https://
71 storefront-eu.example.com/Citrix/StoreWeb/" }
72 , `
73 @{
74 "ServiceTitle" = "StoreFront US"; "StoreWebAddress" = "https://
75 storefront-us.domain.com/Citrix/StoreWeb/" }
76 , `
77 @{
78 "ServiceTitle" = "StoreFront APAC"; "StoreWebAddress" = "https://
79 storefront-apac.domain.com/Citrix/StoreWeb/" }
80
81 # Remove the existing Fallback configuration
82 Remove-WorkspaceFallbackConfiguration -WorkspaceUrl $YourCustomerURL `
83 -ClientId $YourCustomerAPIKey `
84 -ClientSecret $YourCustomerSecretKey `
85 -Verbose
86 <!--NeedCopy-->
```

## Additional help and support

For troubleshooting help or questions, contact your Citrix sales representative or [Citrix Support](#).

## Optimize workflows

May 17, 2021

Simplify valuable workflows with Citrix Workspace, harnessing microapp technology with out-of-the-box templates available today. These use cases give employees a consistent and modern experience independent of the legacy systems they leverage, providing a simplified and effective way to perform important departmental workflows.

### IT Self-service

IT Self-service workflows enable employees to quickly find the IT resources that they need, when they need them. Leveraging this new portfolio of IT Self-service microapps within the workspace, organizations can reduce time spent by employees on IT tasks, improve overall employee NPS for IT services, and reduce IT case volume.



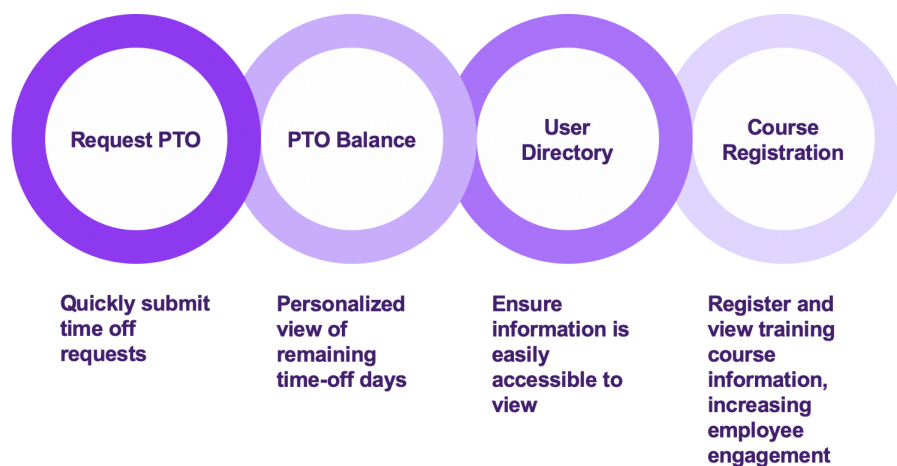
This use case is available through the Microapps service via our out-of-the-box template integrations with:

- ServiceNow integration: Submit Incident microapp and Incidents microapp
- Zendesk integration: Add Ticket microapp and Tickets microapp
- Jira: Create Ticket microapp and Tickets microapp

To find out more, see [IT Self-service](#).

## HR Self-service

It is more essential than ever that businesses rethink their people strategies, placing new emphasis on delivering a best-in-class employee experience that differentiates and elevates the business. Using this new portfolio of HR self-service microapps within the workspace, organizations can improve process efficiency, time savings and reduce HR case volume.



This use case is available through the Microapps service via our out-of-the-box template integrations with:

- Workday integration: Create PTO Request microapp and PTO Balance microapp
- SAP SuccessFactors: Directory microapp and Learning microapp
- Kronos Workforce Central: Request Time Off microapp and My Accrual Balance microapp

To find out more, see [HR Self-service](#).

## Sales Productivity

Your Sales teams are critical to your organization. Empower them to spend more time driving business, and less time searching for information and inputting notes across multiple systems. Using the new Sales Productivity microapps within the workspace, organizations can accelerate time-to-close through greater account insights, increase visibility of sales exceptions and process delays, and reduce time spent on administrative tasks. Simplify workflows like lead creation, opportunity conversion, and task management.



This use case is available through the Microapps service via our out-of-the-box template integrations with:

- Salesforce integration: Create Lead, Create Contact, Create Contract, Create Opportunity, Create Task, Contracts, and Opportunities microapps
- MS Dynamics CRM integration: Create Lead, Create Contact, Create Opportunity, Create Task, and Opportunities microapps

To find out more, see [Sales Productivity](#).

## Employee Well-being

Deliver a workspace that integrates well-being into the way people like to work. There's no doubt that employees can benefit from well-being tools that help them manage the stress and complexities of the workday. The challenge is getting those tools to employees without adding yet another item to their to-do list. Teams can use Citrix Workspace technology to improve the overall employee experience by delivering well-being tools and resources within an intelligent feed.



This use case is available through the Microapps service via our out-of-the-box template integrations with Citrix Podio. Available microapps include:

- Broadcast microapps – Customize and send a dynamic message to employees' intelligent feeds.
- FAQ microapp – Compile a list of FAQs or table of information, communicated and expandable within employees' intelligent feeds.

To find out more, see [Employee Well-being](#).

## Video resources

Check out these videos for demos of these workflows:

[IT Self-service microapp Demo](#)

[HR Self-service microapp Demo](#)

[Sales Productivity microapp Demo](#)

[Employee Well-being Demo](#)

## IT Self-service

February 8, 2021

Both end users and IT service desks experience frustration due to recurring and minor IT tickets and incidents. Organizations are facing increasingly costly and inefficient IT caseloads due to the wide variety of tools and technologies that employees need. Meanwhile employees simply want to be able to resolve their incidents as quickly as possible to maintain their productivity.

With Citrix Workspace, companies can provide a consistent work experience on any device. This enables employees to quickly find the IT resources that they need, when they need them. Leveraging a new portfolio of IT self-service microapps within the workspace, organizations can reduce time spent by employees on IT tasks, improve overall employee NPS for IT services, and reduce IT case volume.

Citrix Workspace is unique in its ability to offer an indistinguishable experience to users regardless of location or device. It's always the same, ensuring that employees remain productive and secure. To help you get started, we have identified specific IT self-service workflows that results in improved employee productivity and employee satisfaction.

## Workflows

This use case is available through the Microapps service via our out-of-the-box template integrations with ServiceNow, Zendesk, and JIRA and addresses these workflows:

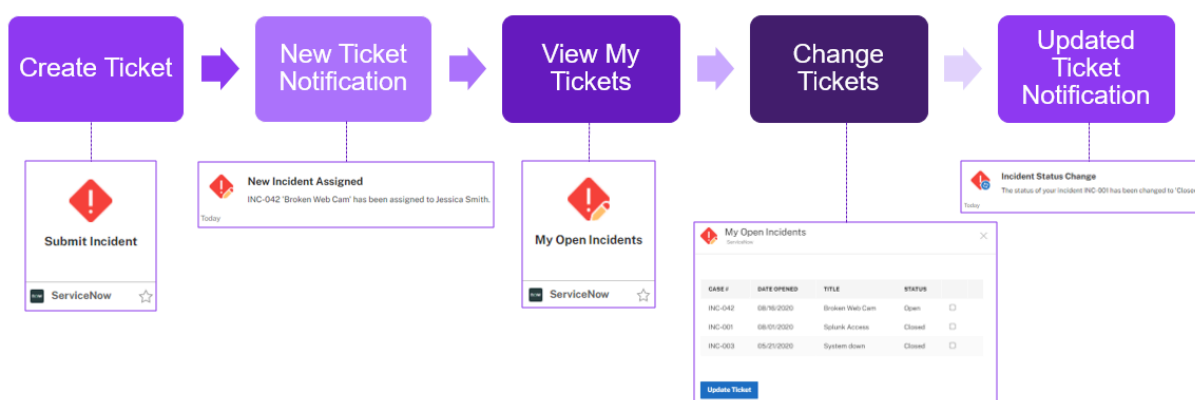


**Submit Incident** – Quickly request help when you need it.

**Incident Ownership** - Maintain employee productivity with a notification when an incident is assigned.

**Incident Updates** – Decreased time to resolution through notifications with updated information.

**My Open Incidents** – Easily find open incidents that you request, report, or are assigned to.



## Integrations and microapps

You can use this use case with any of these integrations.

### ServiceNow

Set up the [ServiceNow integration](#) to get started. [Manage subscribers](#) for these microapps to enable the workflow:

- Enable **Submit Incident microapp** to submit a new incident.
- Enable **Incidents microapp** to search incidents, view their details, add comments, and update them.

### Zendesk

Set up the [Zendesk integration](#) to get started. [Manage subscribers](#) for these microapps to enable the workflow:

- Enable **Add Ticket microapp** to submit Zendesk tickets.
- Enable **Tickets microapp** to view Zendesk tickets with details.

## Jira

Set up the [Jira integration](#) to get started. [Manage subscribers](#) for these microapps to enable the workflow:

- Enable **Create Ticket microapp** to create a new Jira ticket with details.
- Enable **Tickets microapp** to view tickets, add comments, create subtasks, and change status and assignee.

## Video resource

Check out this video for a demo of this use case:

[IT Self Service microapp Demo](#)

## HR Self-service

May 26, 2021

Today's workers remain plagued by endless stacks of apps and logins. They spend the equivalent of a full workday each week searching systems and hunting down information, and fail to take advantage of available company benefits.

It is more essential than ever that businesses rethink their people strategies by placing new emphasis on delivering a best-in-class employee experience that differentiates and elevates the business. Leveraging a new portfolio of HR self-service microapps within the workspace, organizations can improve process efficiency, time savings, and reduce HR case volume.

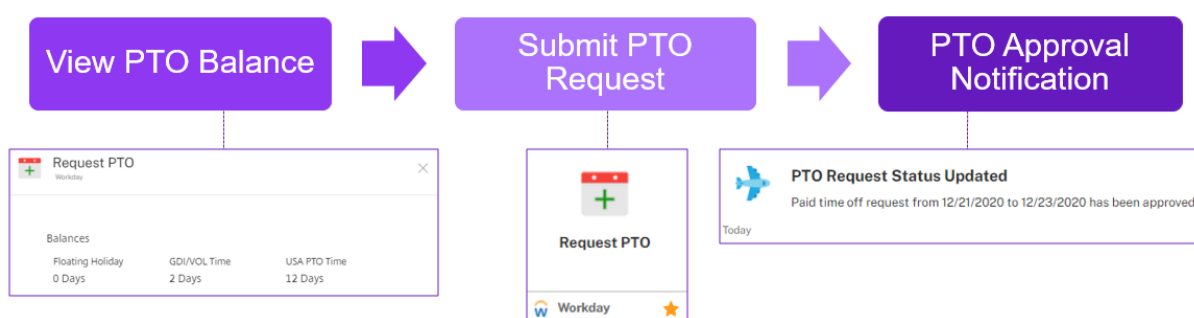
Citrix Workspace is unique in its ability to offer an indistinguishable experience to users regardless of location or device. It's always the same, ensuring that employees remain productive and secure. To help you get started, we have identified specific HR self-service workflows that results in improved process efficiency, time savings, and reduced HR case volume.

## Workflows

This use case is available through the Microapps service via our out-of-the-box template integrations with Workday and SAP SuccessFactors and addresses these workflows.

**Request PTO** – Quickly submit time off requests.

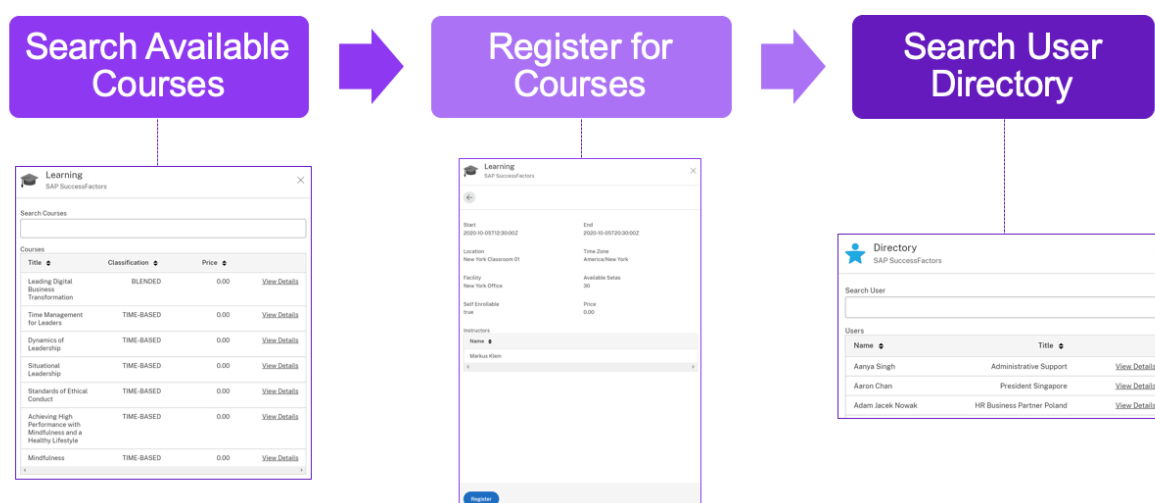
**PTO Balance** - Personalized view of remaining time-off days.



**Users** – Provides a table view of users with search functionality and a link to user details.

**Courses** - Provides a list of available courses with a link to learning item details.

**Scheduled Offering Detail** – Detailed view of a scheduled offering with a list of instructors and an option to register for the offering.



## Integrations and microapps

This use case requires these integrations and the following microapps.

### Workday

Set up the [Workday integration](#) to get started. [Manage subscribers](#) for these microapps to enable the workflow:

- Enable Create PTO Request microapp to submit a paid time-off (PTO) request.
- Enable PTO Balance microapp to view a personalized list of remaining time-off days.

## **SAP SuccessFactors**

Set up the [SAP SuccessFactors integration](#) to get started. [Manage subscribers](#) for these microapps to enable the workflow:

- Enable Directory microapp to search, view, and edit employees with corresponding details.
- Enable Learning microapp to search, view, share, and register available learning courses.

## **Kronos Workforce Central**

Set up the [Kronos Workforce Central integration](#) to get started. [Manage subscribers](#) for these microapps to enable the workflow:

- Enable Request Time Off microapp to submit an application for time off.
- Enable My Accrual Balance microapp to view accrual balance for different days instantly.

## **Video resource**

Check out this video for a demo of this use case:

[HR Self Service microapp Demo](#)

## **Sales Productivity**

March 23, 2021

Sales teams are critical to your organization's success, but sales reps have shared that they are only spending 34% of their time selling because the rest of their time is spent logging activities, searching for information, and inputting sales updates in multiple places.

Empower your sales teams with a new portfolio of Sales Productivity microapps within the workspace, where reps can accelerate time-to-close with personalized notifications, reduce time spent on logging activities, and find the information that they need when they need it.

Citrix Workspace is unique in its ability to offer an indistinguishable experience to users regardless of location or device. It's always the same, ensuring that employees remain productive and secure. To help you get started, we have identified specific Sales Productivity workflows that result in improved process efficiency, time savings, and a great employee experience on any device.

## **Workflow**

This use case is available through the Microapps service via our out-of-the-box template integrations with Salesforce and MS Dynamics CRM, and addresses these workflows:

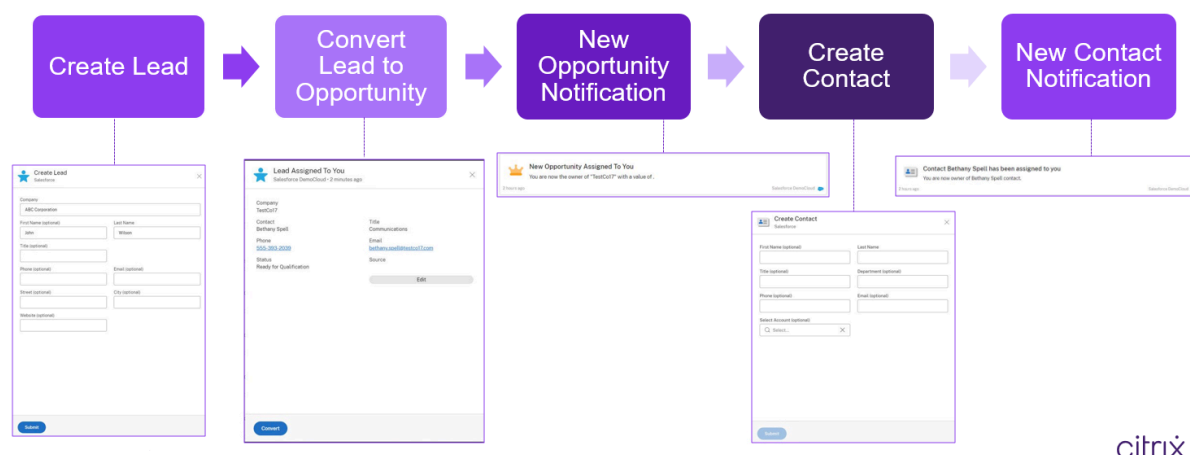
**Opportunity Updates** – Quickly edit opportunity and view opportunity details.

**Task Management** – Improve productivity with real-time notifications.

**Contract Approvals** – Reduce time to close by receiving updates and submitting needed edits.

**Activity Logging** – Streamline efficiencies by logging presales activities and calls.

**Search** – Personalized search experience for sales related admin tasks.



citrix

## Integrations and microapps

You can use this use case with any of these integrations.

### SalesForce

Set up the [SalesForce integration](#) to get started. [Manage subscribers](#) for these microapps to enable the workflow:

- Enable **Create Lead** to provide a form for submitting a new lead
- Enable **Convert Lead** to provide a form for converting a lead
- Enable **Create Contact** to provide a form for submitting a new contact
- Enable **Opportunity Assigned To You (New)** notification for a user to receive a notification when a new opportunity is assigned to the user
- Enable **Account Assigned to You (New)** notification for a user to receive a notification when a new account is assigned to the user

### MS Dynamics CRM

Set up the [MS Dynamics CRM](#) to get started. [Manage subscribers](#) for these microapps to enable the workflow:

- Enable **Create Lead** to provide a form for submitting a new lead
- Enable **Create Contact** to provide a form for submitting a new contact
- Enable **Opportunity Assigned To You (New)** notification for a user to receive a notification when a new opportunity is assigned to the user
- Enable **Account Assigned to You (New)** notification for a user to receive a notification when a new account is assigned to the user

## Video Resource

Check out this video for a video on Workspace for Sales Teams:

[Sales Productivity microapp Demo](#)

## Employee Well-being

February 9, 2021

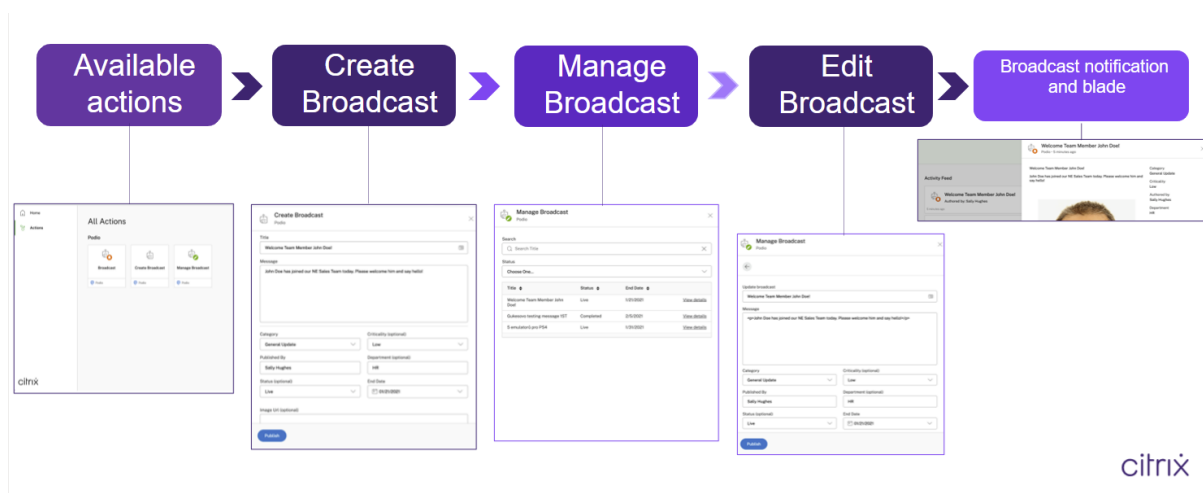
Deliver a workspace that integrates well-being into the way people like to work. There's no doubt that employees can benefit from well-being tools that help them manage the stress and complexities of the workday. The challenge is getting those tools to employees without adding yet another item to their to-do list. Teams can use Citrix Workspace technology to improve the overall employee experience by delivering well-being tools and resources within an intelligent feed.

## Workflow

This solution is available through the Microapps service using our out-of-the-box template integrations with Citrix Podio. This can also act as a system of record across Citrix Workspace use cases, including employee well-being:

**Employee Resources** – Surface relevant content and FAQs to support employees with our FAQs microapp.

**Good News** – Increase employee morale by sharing positivity across your organization with our Broadcast microapps.



## Citrix Podio integration template and microapps

Our Citrix Podio integration template provides these out-of-the-box microapps. Set up the [Citrix Podio integration](#) to get started. [Manage subscribers](#) for these microapps to enable the workflow:

**Broadcast app** – Customize and send a dynamic message to employees' intelligent feeds.

- Enable **Broadcast microapp** to view all published broadcasts.
- Enable **Create Broadcast microapp** to create and publish new broadcasts.
- Enable **Manage Broadcast microapp** for administrators to view and update all created broadcasts.

**FAQs app** – Compile a list of FAQs or table of information, communicated and expandable within employees' intelligent feeds.

- Enable **FAQs microapp** to list of commonly asked questions and answers and view details.

Check out the [Employee Well-Being App Pack](#) for more inspirational ideas.

Besides these Citrix well-being microapps, the Workspace experience is open for you to integrate your own well-being vendor and platform to surface as quick actions where work gets done. Applications can be customized to suit your organization's needs and unique processes. Advanced workflow automation capabilities are available to trigger custom email updates, approvals, and intelligent workflows on top of the actions and feed cards in Workspace.

## Video resource

Check out this video for a demo of how Citrix Workspace can be infused with the employee well-being use case via Citrix Podio:

[Employee Well-being Demo](#)

**Locations**

Corporate Headquarters | 851 Cypress Creek Road Fort Lauderdale, FL 33309, United States  
Silicon Valley | 4988 Great America Parkway Santa Clara, CA 95054, United States

© 2021 Citrix Systems, Inc. All rights reserved. Citrix, the Citrix logo, and other marks appearing herein are property of Citrix Systems, Inc. and/or one or more of its subsidiaries, and may be registered with the U.S. Patent and Trademark Office and in other countries. All other marks are the property of their respective owner(s).