Citrix Workspace

Contents

Citrix Workspace

May 28, 2020

Citrix Workspace is a complete digital workspace solution that allows you to deliver secure access to the information, apps, and other content that are relevant to a person's role in your organization. Users subscribe to the services you make available and can access them from anywhere, on any device. Citrix Workspace helps you organize and automate the most important details your users need to collaborate, make better decisions, and focus fully on their work.

For a complete description of each Citrix Workspace edition and included features, see the Citrix Workspace Feature Matrix.

Get started

Citrix Workspace includes a step-by-step walkthrough to help you deliver workspaces quickly. Each step guides you through the Citrix Cloud console with simple instructions for tasks like configuring your identity provider, selecting your workspace authentication, and enabling the other services that come with Workspace. The walkthrough also provides quick access to the technical information you'll need when you're assembling your deployment team and configuring your infrastructure and resources. For an overview of the tasks you'll perform and the information you'll need as you progress in your deployment, see Get Started with Citrix Workspace.

Microapps

Microapps helps you deliver relevant, actionable notifications from your applications directly into users' workspaces. Build integrations from your application data sources to pull actions into Workspace. Microapps can write back to source systems, so users can address these actions without leaving their workspace. Users save time and can focus on their primary work because they don't have to switch to other applications to interact with key business systems in your organization.

For more information, see the Microapps service documentation.

Citrix Virtual Apps Essentials service

Citrix Virtual Apps Essentials offers secure access to virtual Windows apps. This service includes a workspace URL, enabled by default, usually in the format: `https://yourcompanyname.cloud.com`. Follow the steps to set up Citrix Virtual Apps Essentials, then test and share the workspace URL link with your subscribers to give them access to their apps.

Citrix Virtual Desktops Essentials service

Citrix Virtual Desktops Essentials offers secure access to Windows 10 virtual desktops. This service includes a workspace URL, enabled by default, usually in the format: `https://yourcompanyname.cloud.com`. Follow the steps to set up Citrix Virtual Desktops Essentials, then test and share the workspace URL link with your subscribers to give them access to their desktops.

Citrix Virtual Apps and Desktops service

The Citrix Virtual Apps and Desktops service offers secure access to virtual apps and desktops. This service includes a workspace URL, enabled by default, usually in the format: `https://yourcompanyname.cloud.com`. Follow the steps to set up the Citrix Virtual Apps and Desktops service, then test and share the workspace URL link with your subscribers to give them access to their apps and desktops. Your subscribers can access the workspace URL without any additional configuration.

Endpoint Management

For Endpoint Management customers with the workspace experience enabled, users who open Secure Hub and click **Add Apps** are directed to the Workspace apps store instead of the Secure Hub store. This feature is available only to **new customers**. Migration for existing customers is not supported. To use this feature, perform the following tasks:

- To deploy the Workspace experience to new devices, add them to the Workspace delivery group. For more information, see Citrix Endpoint Management integration with Citrix Workspace.
- Enable the Password Caching and Password Authentication policies. For more information on configuring policies, see MDX Policies at a glance.
- Configure Active Directory authentication as AD or AD+Cert. These are the two modes that we support. For more information on configuring authentication, see Domain or domain plus security token authentication.
- Enable Workspace integration for Endpoint Management. For more information on workspace integration, see Workspace Configuration.

  > **Important:**
  >
  > After this feature is enabled, ShareFile SSO occurs through Workspace and not through Endpoint Management. We recommend that you disable ShareFile integration in the Endpoint Management console before you enable Workspace integration.

Citrix Gateway service

The Citrix Gateway service (formerly NetScaler Gateway Service) provides secure remote access with Identity and Access Management (IdAM) capabilities, delivering a unified experience to SaaS (Software as a Service) apps and virtual apps and desktops. Follow the steps to set up the Citrix Gateway service, then test and share the workspace URL with your subscribers to give them remote access. For more information on configuring SaaS apps within the Citrix Gateway service, see Support for Software as a Service Apps.

Content Collaboration service

The Content Collaboration service (formerly ShareFile) provides secure data access, sync, and sharing of files from any device. Follow the steps to set up the Content Collaboration service, then test and share the workspace URL with your subscribers to give them access to Files.

Secure Browser service

The Secure Browser service protects the corporate network from browser based attacks by isolating web browsing. When subscribers (users) navigate to the URL provided by the administrator, their published browsers are shown, along with other apps and desktops that are configured for them in other Citrix Cloud services. Follow the steps to set up the Secure Browser Service, then test and share the workspace URL with your subscribers to give them access to a secure browser.

Example use case

Your organization currently manages a mix of Microsoft Office apps through the Citrix Virtual Apps and Desktops service and SaaS apps such as Workday through the Citrix Gateway service.

You also have legacy apps from an on-premises Virtual Apps and Desktops deployment. You can now deliver all these apps into a single integrated user experience.

The user can access their workspace with all the apps they need from a browser or app - the **Citrix Workspace app**. You can customize the experience in a simplifed console (**Workspace Configuration**) in Citrix Cloud, and choose how you want users to authenticate.

For this use case, complete the set up for the individual **services** first. Switch to **Workspace Configuration** to carry out further customization and configuration to the overall behavior of the Workspace user experience. Workspace Configuration (in the **Sites** tab) is also where you connect up your on-premises Virtual Apps and Desktops deployment to the Workspace user experience (known as *Site aggregation*). Share the **Workspace URL** with your users for clientless access, and guide them to install the **Citrix Workspace app** for the best experience.

Copied!
Failed!

What's New

June 19, 2020

A goal of Citrix is to deliver new features and updates to Citrix Workspace customers when they are 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 in waves helps ensure product quality and maximize 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.

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.

March 2020

Citrix Assistant: Citrix Assistant is a virtual assistant now available with Citrix Workspace. It provides an easy medium to accomplish tasks such as viewing employee information, finding expense reports, and finding tickets. The Citrix Workspace virtual assistance feature improves employee engagement and productivity by providing immediate access to relevant content and business data. The virtual assistant pulls data from connected applications and helps you quickly find the information you need. It uses automated intelligence, machine learning capabilities, and natural language processing to understand the app context, conversation context, and user intent. For more information, see Citrix Assistant

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 (Technical Preview): 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.

Copied!
Failed!

Get Started with Citrix Workspace

May 21, 2020

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: Internet 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.
  - Citrix Assistant describes how you can help your end-users find answers to commonly-asked questions more quickly with Citrix Assistant's machine learning and natural language processing capabilities.
- Endpoint Management: Onboarding and resource setup
- Virtual Apps and Destops: 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
- Asking a question with Citrix Assistant and verifying the correct information is returned

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.

Copied!
Failed!

Citrix Workspace app and Citrix Receiver

February 25, 2020

Citrix recommends that Workspace subscribers use the latest version of Citrix Workspace app.

You can also access workspaces using Internet Explorer 11, or the latest version of Edge, Chrome, Firefox, or Safari.

Currently, some customers continue to use Citrix Receiver. Citrix Receiver is supported for any of the desktop platforms (Windows, Mac, and Linux). Citrix Receiver for HTML5 and Citrix Receiver for Chrome are also supported.

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

Supported authentication methods for Citrix Workspace app

The following table shows the authentication methods supported by Citrix Workspace app.

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.

Citrix Receiver and 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

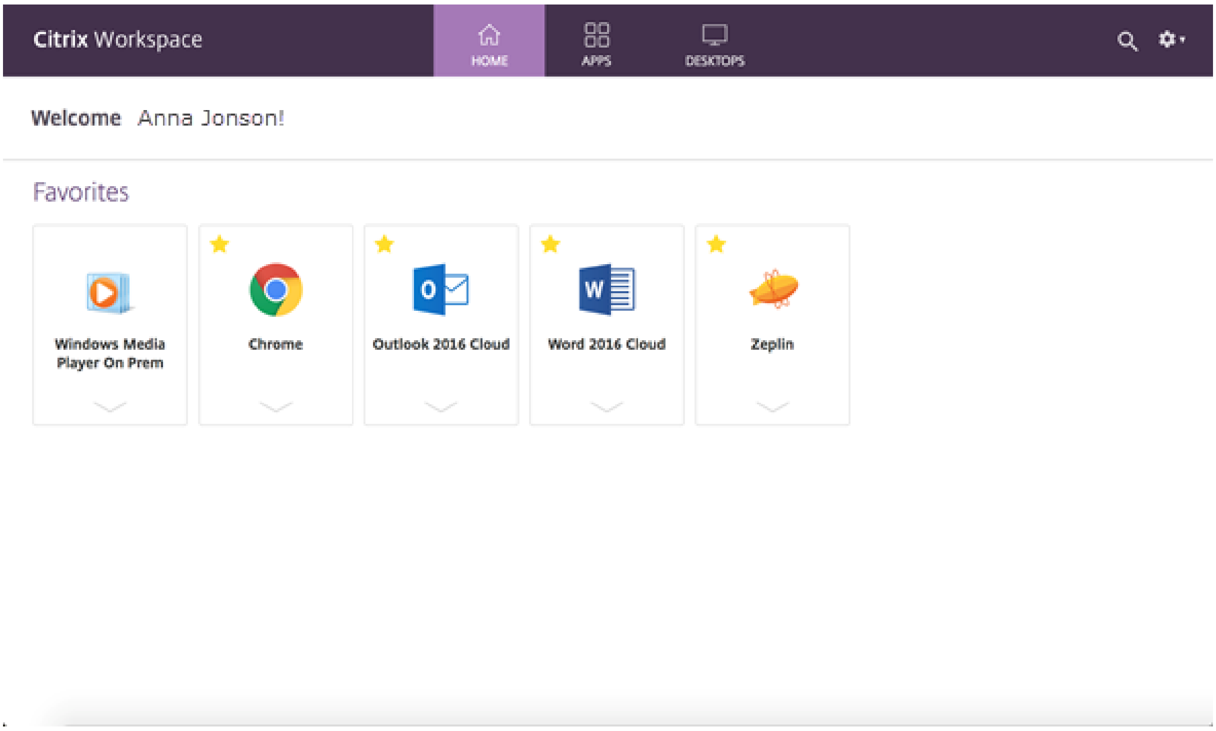
New customers. If you are new to the workspace experience, you'll get the latest version of the user interface as soon as it is available. You can access the workspace experience from your browser or from a local Citrix Workspace app.

Existing customers. If you have been working with an earlier version of Citrix Workspace, it can take around five minutes for the updated user interface 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 have been working with Citrix Receiver as your local app, you will need to guide your users to upgrade to Citrix Workspace app to use all the features of the Citrix Cloud services.

The scenarios below illustrate what users are likely to see.

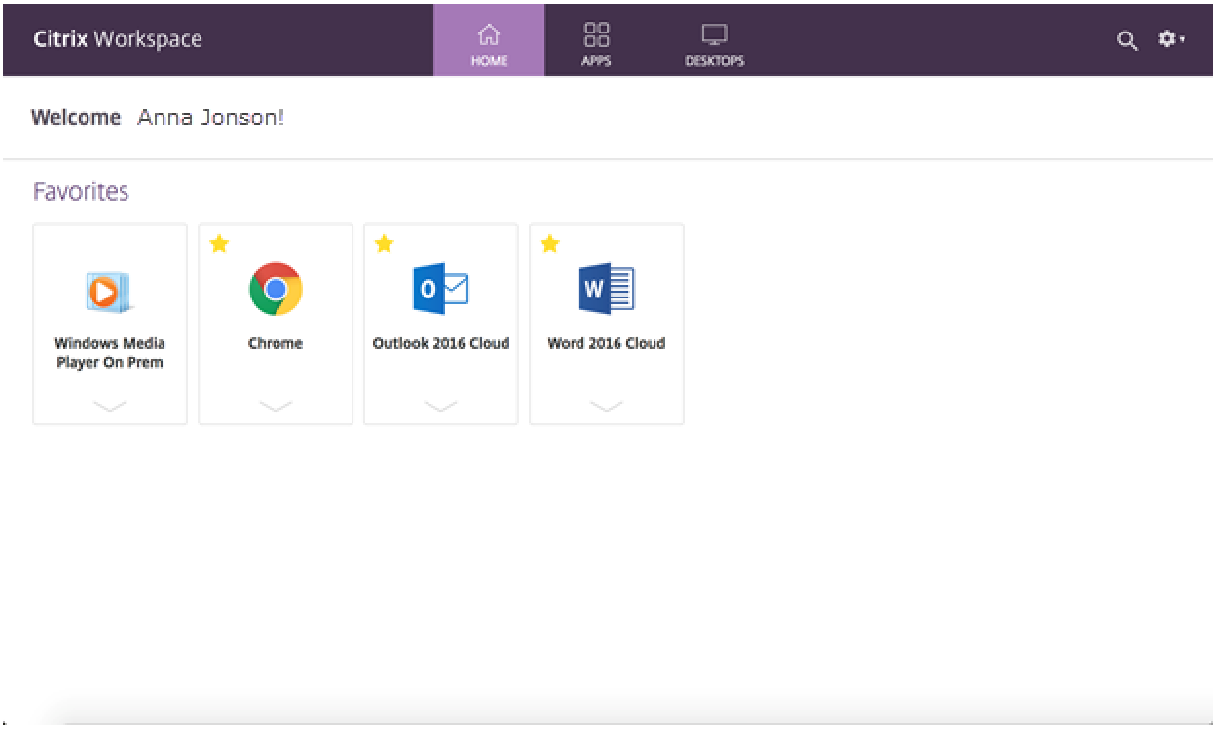
Citrix Receiver

If your users are accessing Workspace with Citrix Receiver, with the above service integrations enabled, users will see the "purple" user interface shown below. They will 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 will not be able to access them this way.



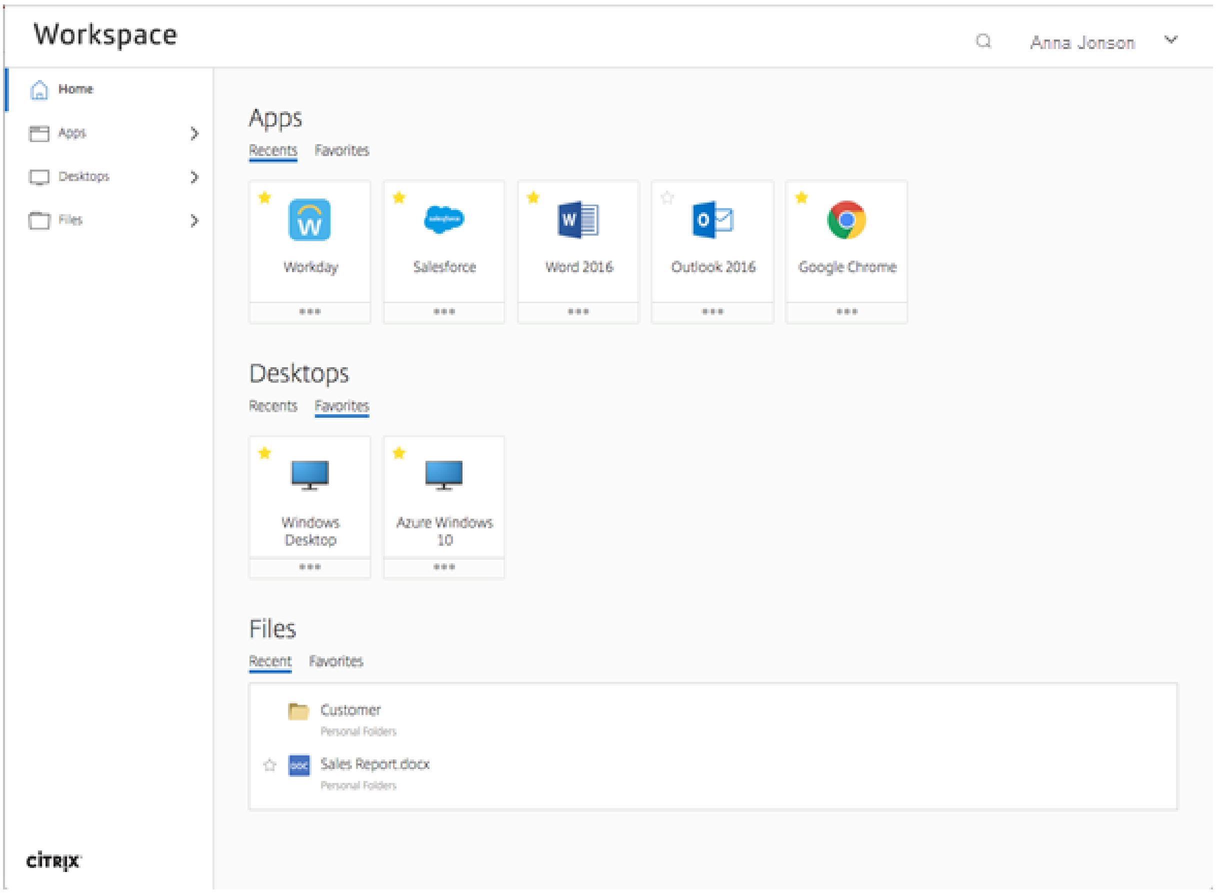
With the same services enabled and **access control** enabled, users will still see the purple user interface, however without web and SaaS apps, as the access control feature is not supported in Citrix Receiver.

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



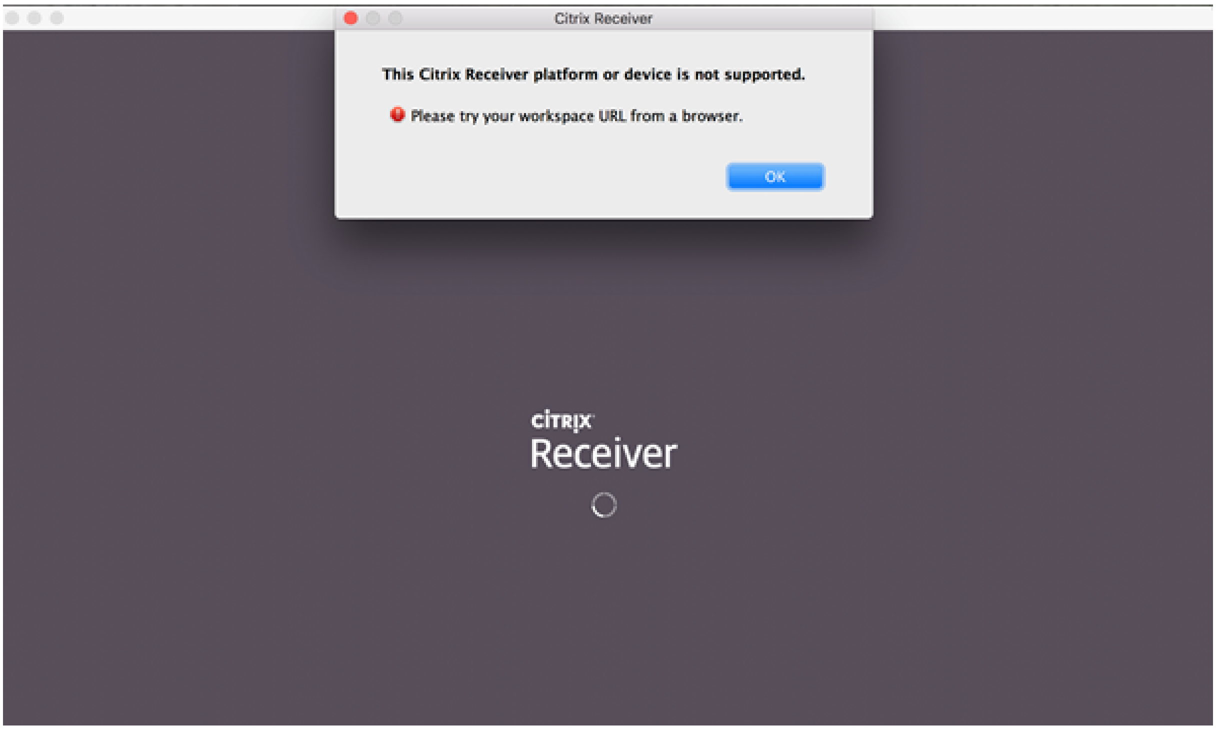
Citrix Workspace app or browser

When your users upgrade to Citrix Workspace app or use a web browser to access Workspace, they will see the new user interface and can use of all the new functionality including Files.



Azure Active Directory (AAD)

This scenario is for either AAD enabled as the Workspace authentication method. If your users try to log on using Citrix Receiver, they will see a message that the device isn't supported and to try from a browser instead. Once they have upgraded to Citrix Workspace app, they can access Workspace.



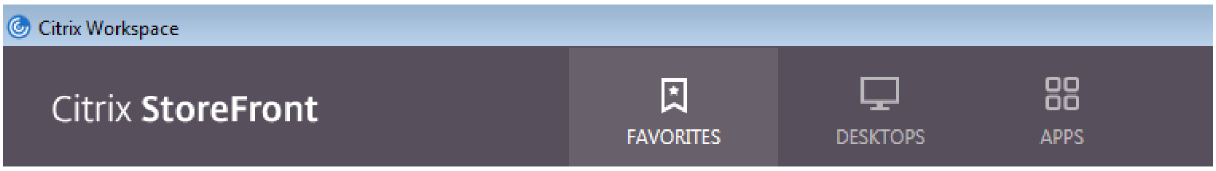
Citrix Receiver

This Citrix Receiver platform or device is not supported.

Please try your workspace URL from a browser.

StoreFront (on-premises deployment)

If you have a StoreFront on-premises environment and 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 use their "purple" user interface when using the Workspace app or when accessing from a web browser.

Copied!
Failed!

Configure workspaces

June 19, 2020

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

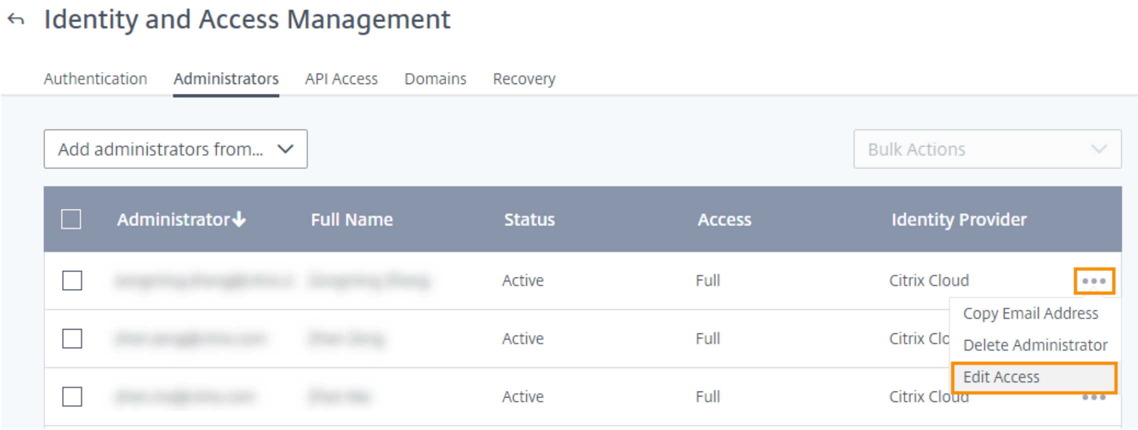
> **Note:**
>
> Looking for workspace authentication articles?
>
> Secure workspaces is the new home for information about supported methods for subscriber authentication to workspaces. See the following sections:
>
> - Active Directory
> - Azure Active Directory
> - Active Directory plus token
> - Citrix 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, click the ellipsis button, and then select **Edit Access**.

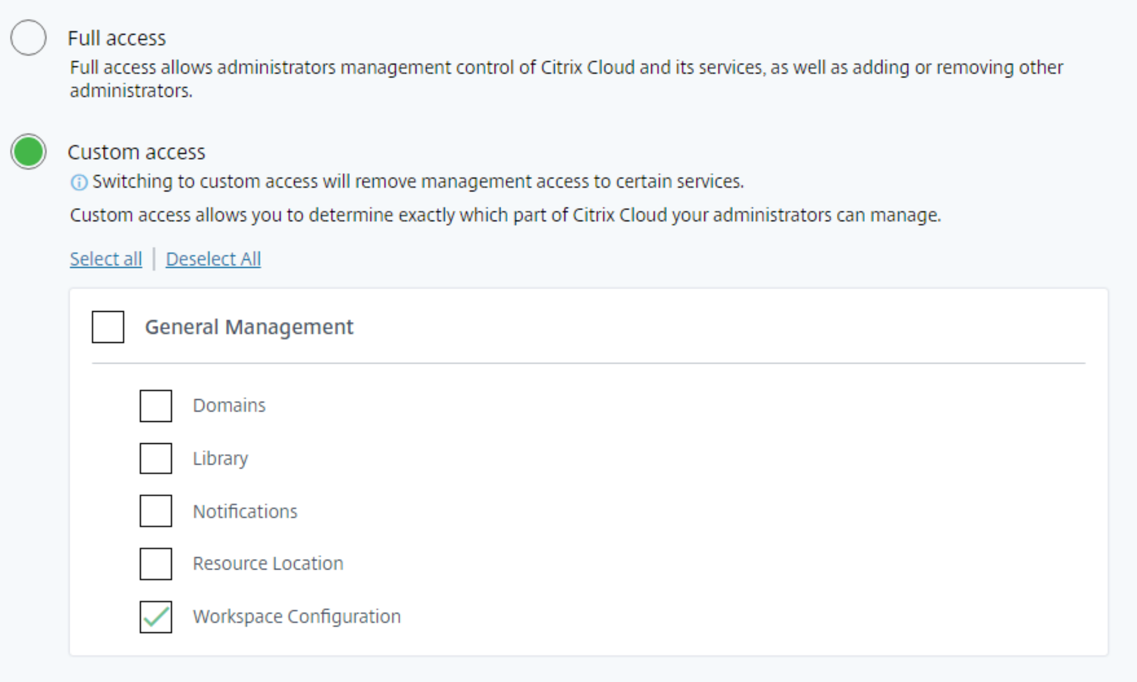


Identity and Access Management

□	Administrator↓	Full Name	Status	Access	Identity Provider
□	[redacted]	[redacted]	Active	Full	Citrix Cloud
□	[redacted]	[redacted]	Active	Full	Citrix Clc
□	[redacted]	[redacted]	Active	Full	Citrix Cloud

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

ⓘ Switching to custom access will remove management access to certain services.

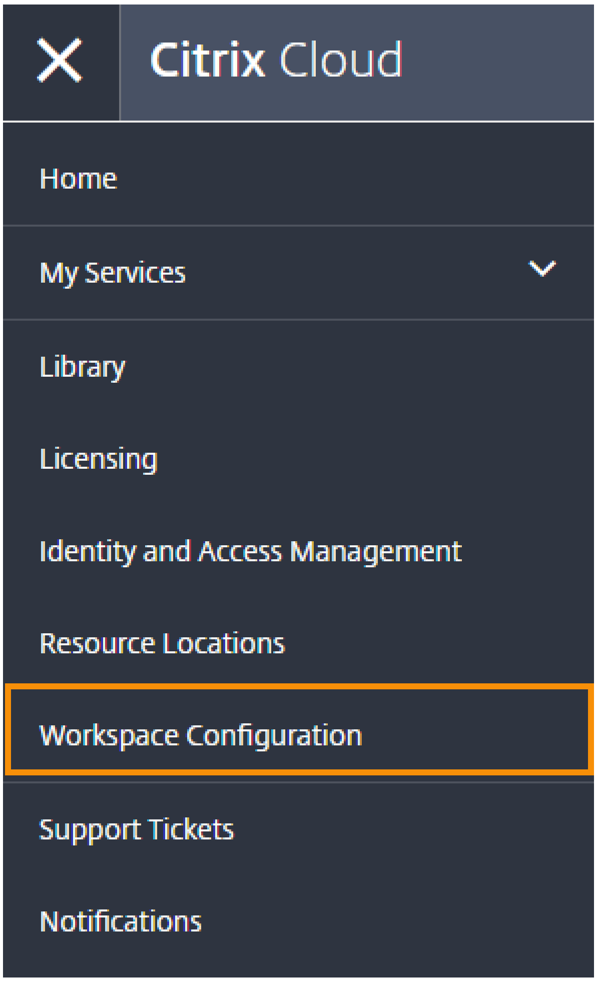
Custom access allows you to determine exactly which part of Citrix Cloud your administrators can manage.

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

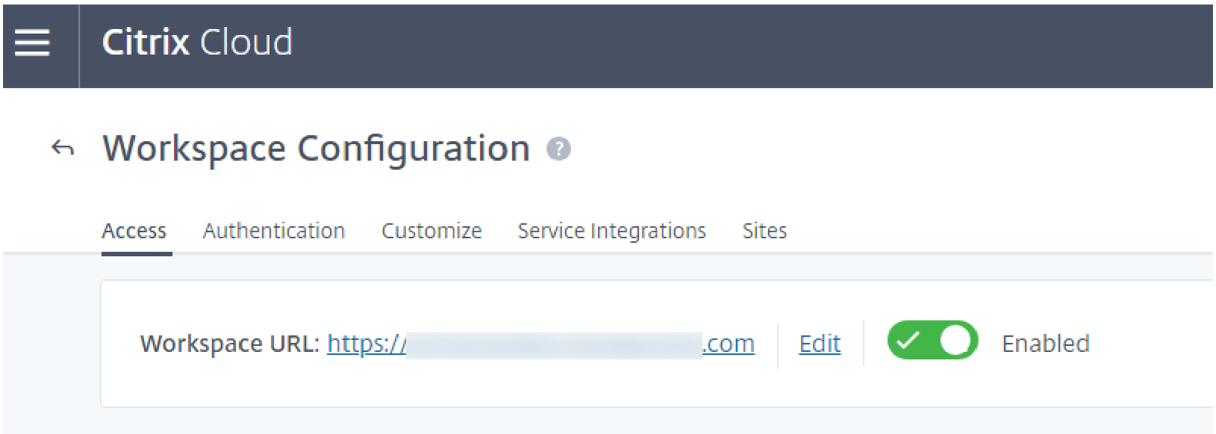
The following addresses must be contactable to operate and consume Citrix Workspace:

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

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

Workspace URL

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



Workspace URL: https://[redacted].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 does not 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 company or organization using the Citrix Cloud account, and must comply with the Citrix End User Services Agreement. Any misuse of a third party’s intellectual property rights including trademarks may result in the revocation and reassignment of the workspace URL and/or the 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.

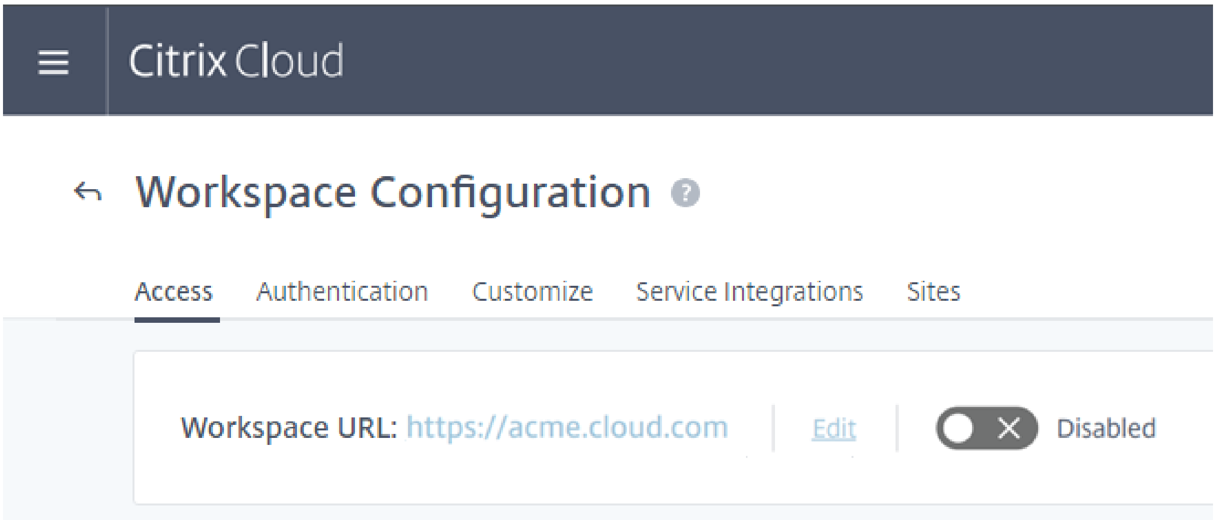
Guidance for new URLs:

- 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, please open a ticket in Citrix Cloud.
- Must consist of only letters and numbers.
- Cannot 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 cannot access their workspaces until the new URL is active (takes about 10 minutes). You'll also need to tell them 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 is 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 subscribers use an on-premises StoreFront URL to access resources or you want to prevent workspace access during maintenance periods.



Workspace URL: https://acme.cloud.com

Disabled

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 will no longer have access to data and applications from all services in Citrix Workspace.
- You cannot customize the workspace URL. You must re-enable the URL before you can change it.

External connectivity

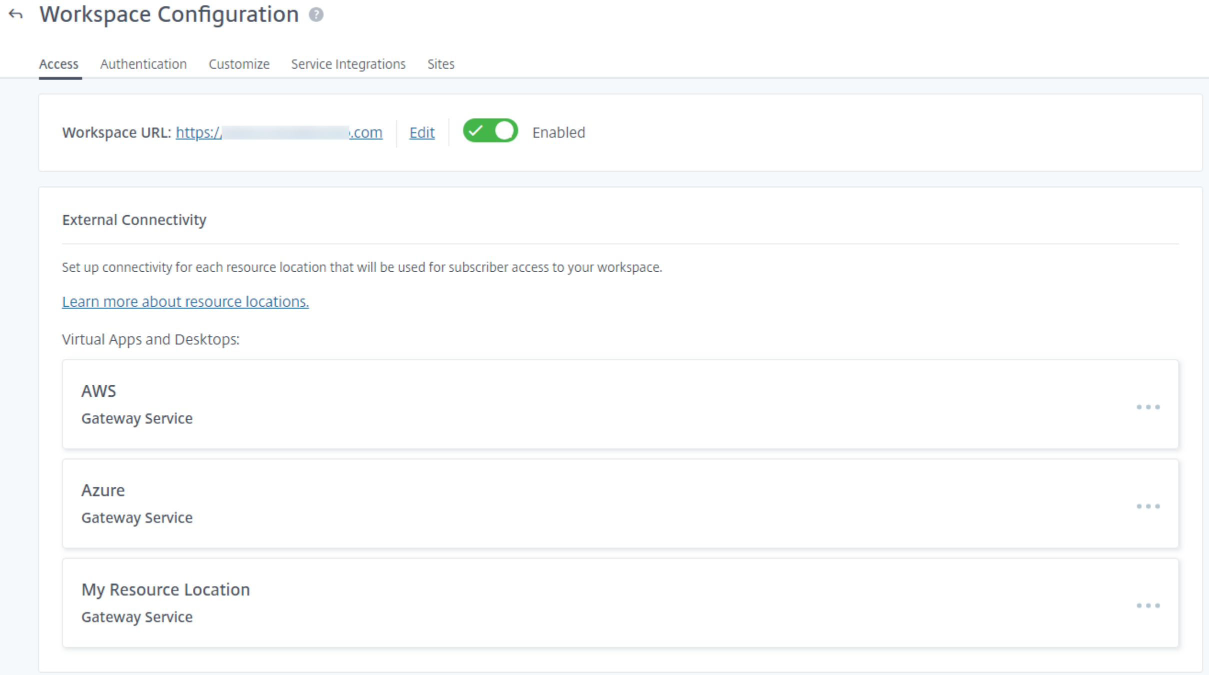
Provide secure access for your remote subscribers by adding Citrix Gateways or the Citrix Gateway service to the resource locations.

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 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 URL: https:/[redacted].com

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 is not 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

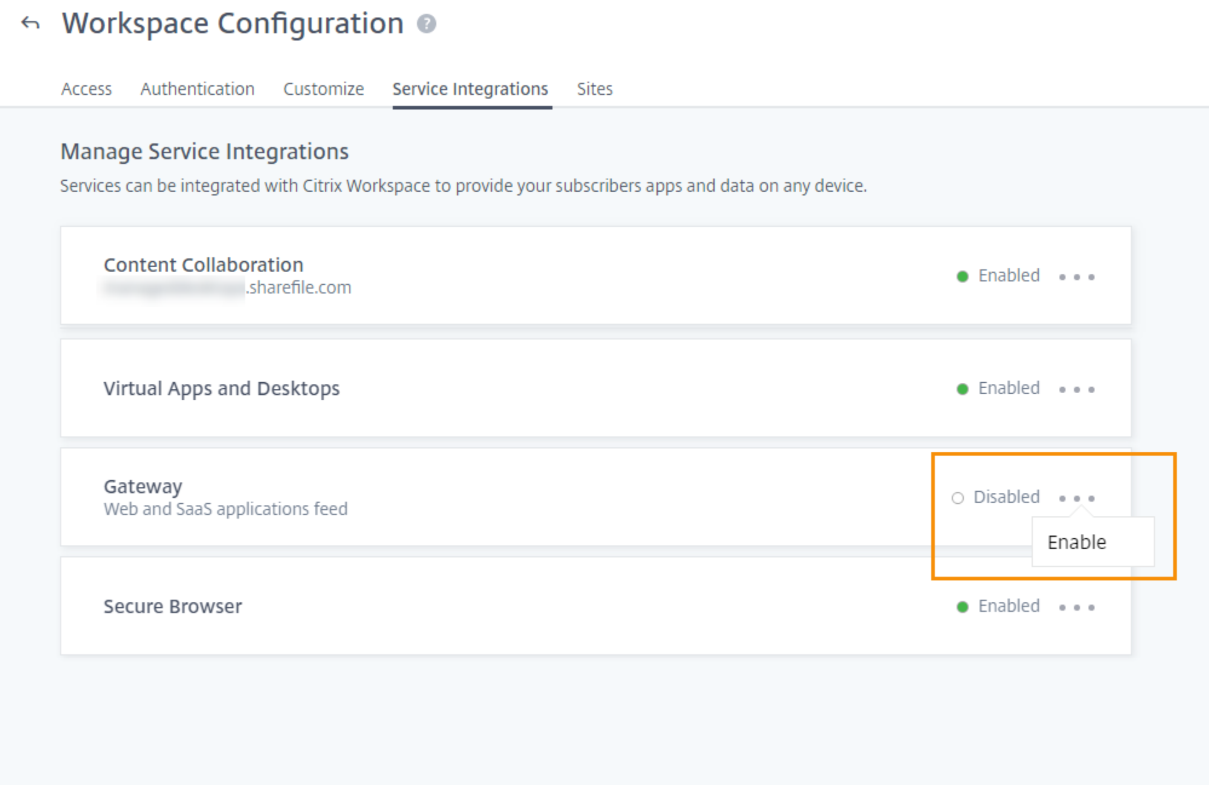
You can enable or disable the availability of individual service resources from the **Service Integrations** tab. By default, the Virtual Apps and Desktops service and the Secure Browser service are enabled after you subscribe to them. All other new services that your organization subscribes to are disabled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

> **Note:**
>
> The 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**.



Manage Service Integrations

Services can be integrated with Citrix Workspace to provide your subscribers apps and data on any device.

Content Collaboration
[redacted].sharefile.com
● Enabled • • •

Virtual Apps and Desktops
● Enabled • • •

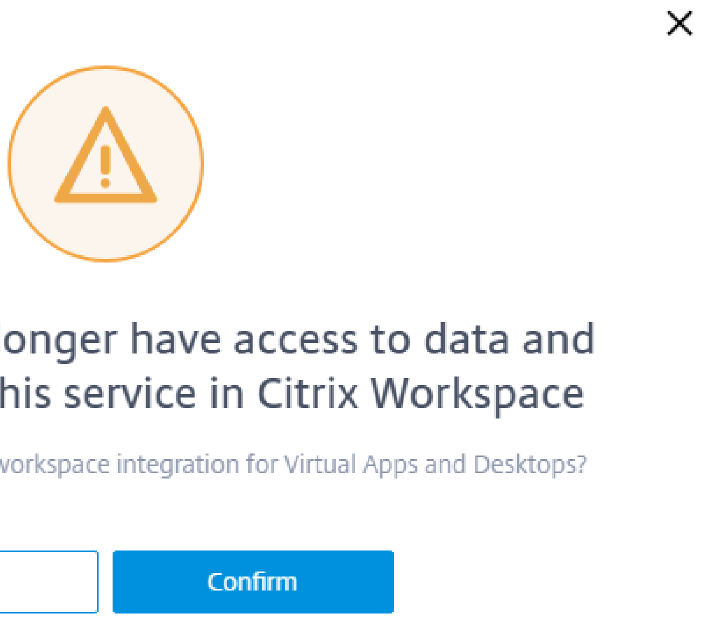
Gateway
Web and SaaS applications feed
○ Disabled • • •
Enable

Secure Browser
● Enabled • • •

To disable workspace integration for a service

> **Important:**
>
> Disabling workspace integration blocks subscriber access for that service. This does not disable the workspace URL, but subscribers will no longer have access to 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 will no longer have access to data or application from the service.

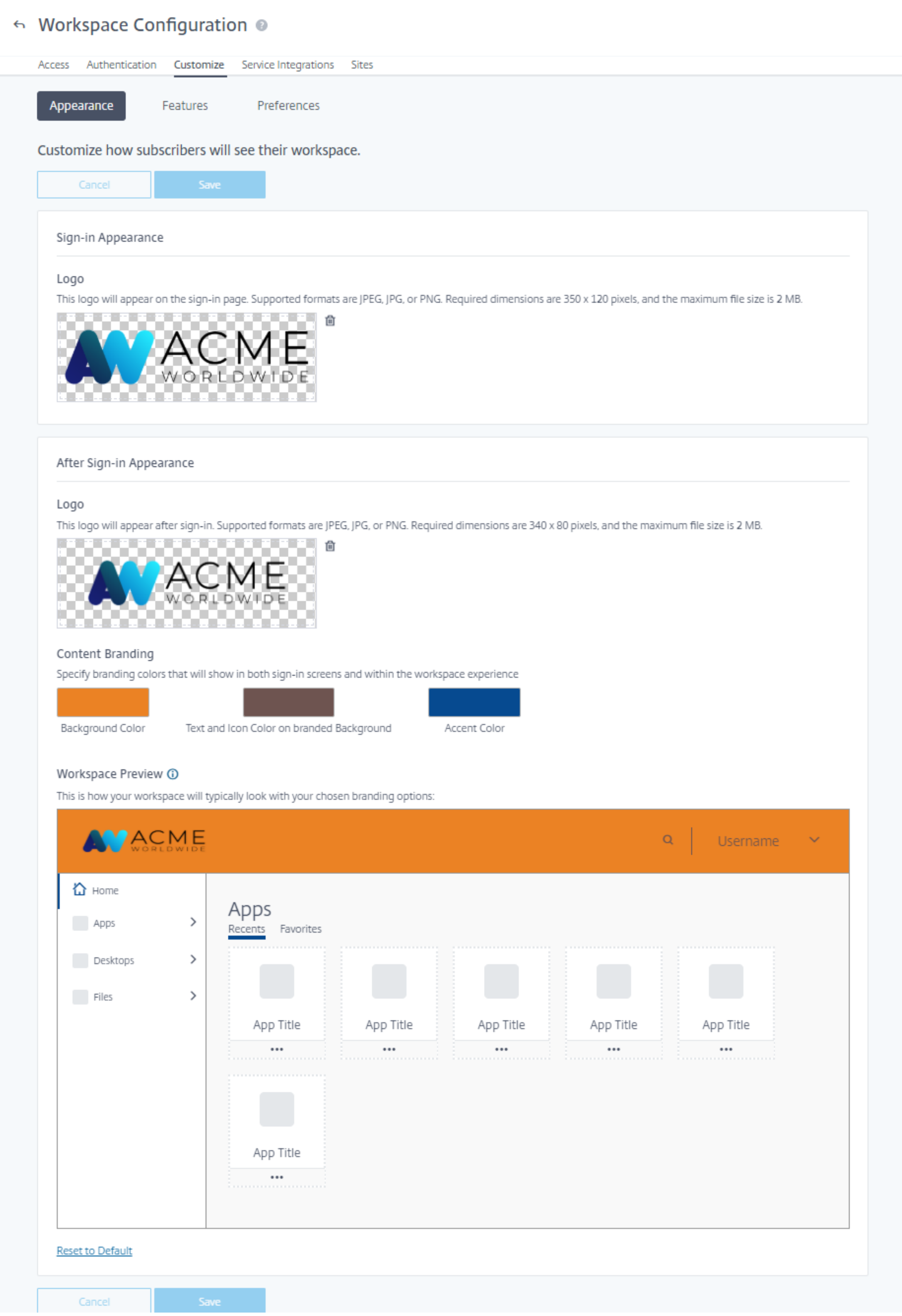


Subscribers will no longer have access to data and applications from this service in Citrix Workspace

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

Customize the appearance of workspaces

To customize how subscribers see their workspace, change the settings in **Workspace Configuration > Customize > Appearance** and **Save**.



Customize how subscribers will see their workspace.

Sign-in Appearance

Logo

This logo will appear on the sign-in page. Supported formats are JPEG, JPG, or PNG. Required dimensions are 350 x 120 pixels, and the maximum file size is 2 MB.

After Sign-in Appearance

Logo

This logo will appear after sign-in. Supported formats are JPEG, JPG, or PNG. Required dimensions are 340 x 80 pixels, and the maximum file size is 2 MB.

Content Branding

Specify branding colors that will show in both sign-in screens and within the workspace experience

Workspace Preview

This is how your workspace will typically look with your chosen branding options:

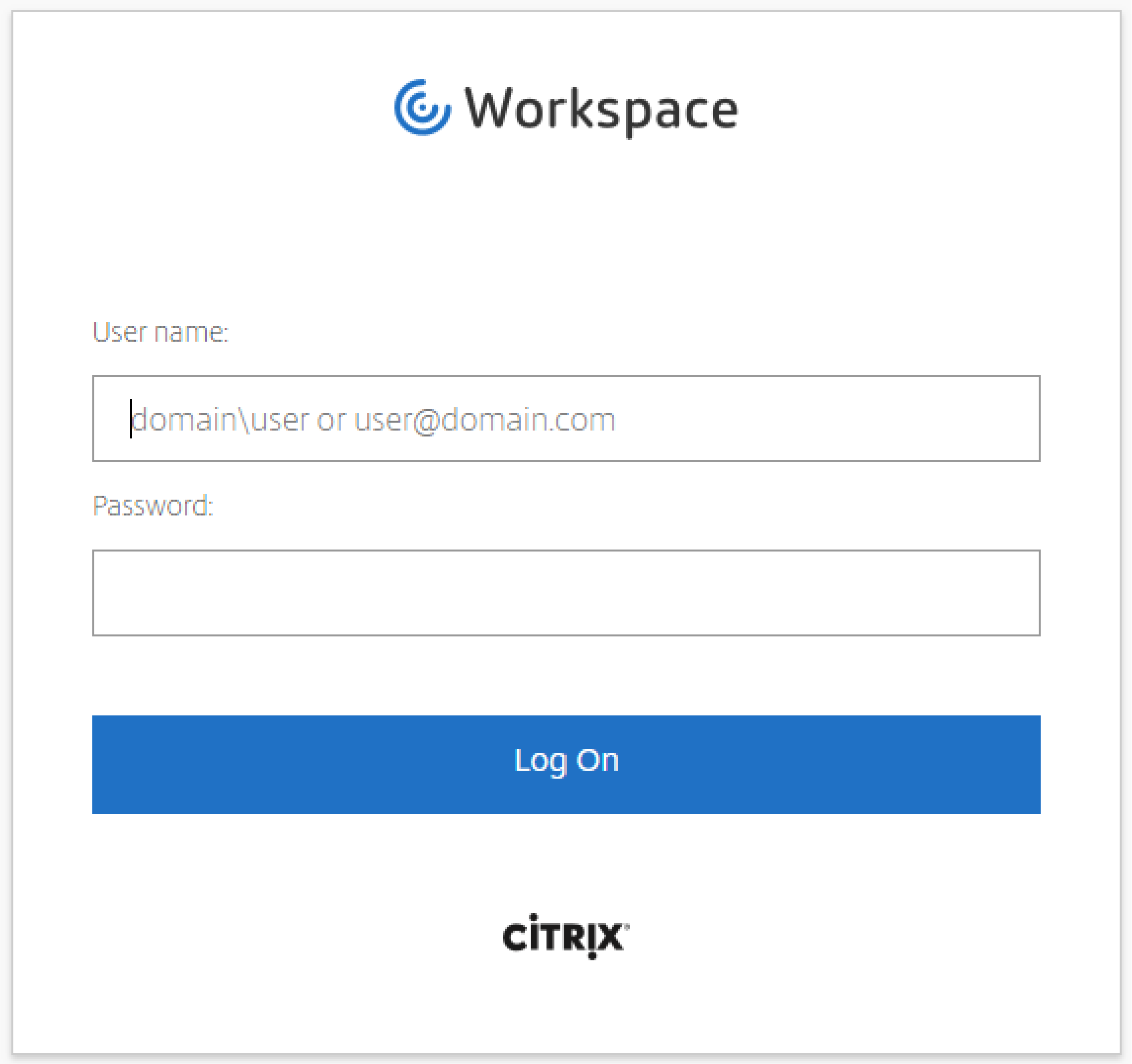
Changes to the workspace appearance take effect right away. Local Citrix Receiver apps may take around five minutes for the updated user interface to display.

> **Note:**
>
> The Workspace Preview does not show a preview if you are currently working with the older "purple" user interface.

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	2MB	JPEG, JPG, or PNG

Logos that do not match the required dimensions may appear distorted.

The **Sign-in** logo appears on the workspace sign-in form. You can replace the Workspace logo with your own. The colors and branding of the rest of the sign-in page are not affected.



Changes to the sign-in logo do not impact users who authenticate to their workspace using Azure Active Directory. For more information on how to add company branding to your sign-in page in Azure AD, see the Microsoft documentation.

The **After Sign-in logo** appears at the top left of the workspace.

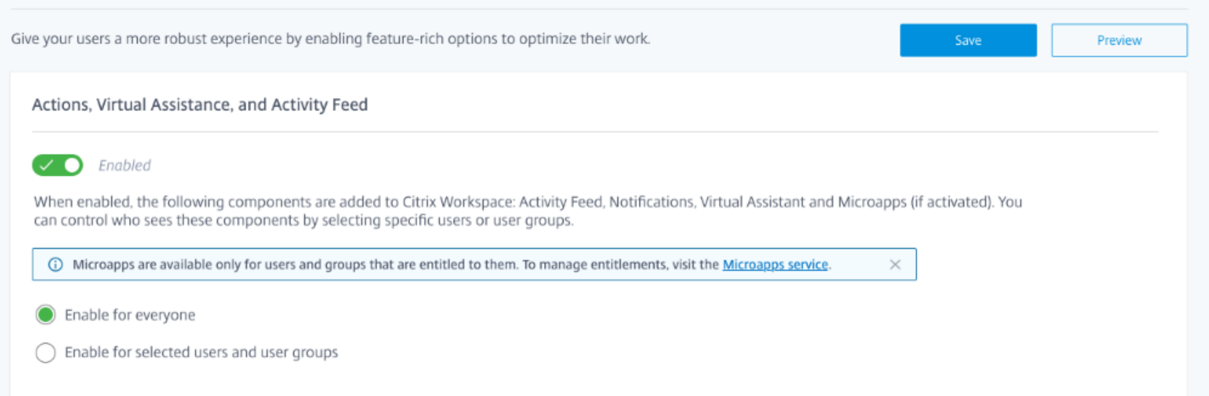
The **Content Branding** colors change the header background, text and icon color, and the accent color in the workspace.

Customize rollout of new features

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

Actions, Virtual Assistance, 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**.



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

Actions, Virtual Assistance, and Activity Feed

Enabled

When enabled, the following components are added to Citrix Workspace: Activity Feed, Notifications, Virtual Assistant and Microapps (if activated). You can control who sees these components by selecting specific users or user groups.

Microapps are available only for users and groups that are entitled to them. To manage entitlements, visit the Microapps service.

● Enable for everyone

○ Enable for selected users and user groups

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 with Citrix Assistant resolvers, subscribers can take action on work items and get quick, automated answers to common workplace queries, all inside their workspace. For more information, see Getting Started in the Microapps documentation.

Requirements for configuration

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

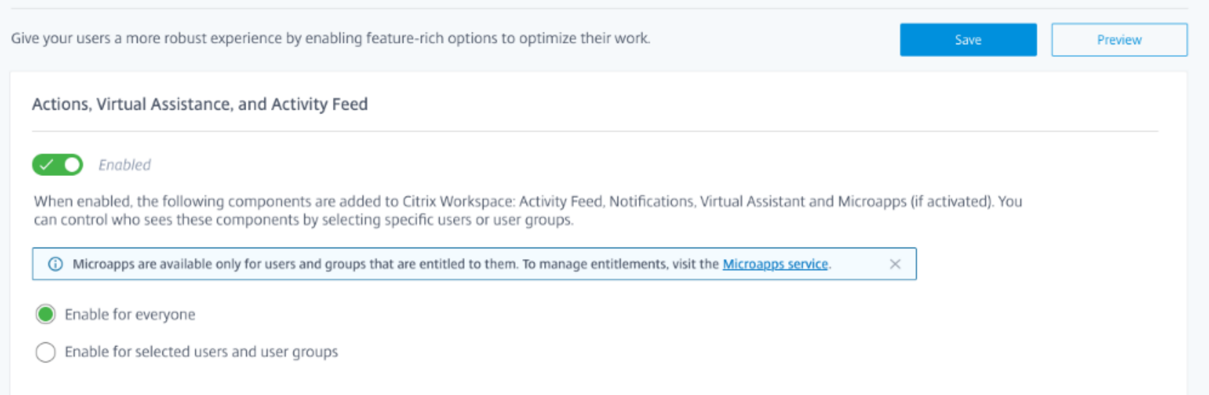
- The Microapps service is enabled in **Workspace Configuration > Service Integrations**.
- You have subscribed the appropriate users and groups to the microapps that will generate actions in the activity feed. For instructions, see Managing subscribers.
- To enable the feature for specific users and 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 are using Citrix Gateway as an identity provider
  - You are using the Citrix Federated Authentication Service with Citrix Cloud.
- To include access to Citrix Assistant when enabling this feature, you must meet the prerequisites described in Citrix Assistant.

Configure the setting

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



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

Actions, Virtual Assistance, and Activity Feed

Enabled

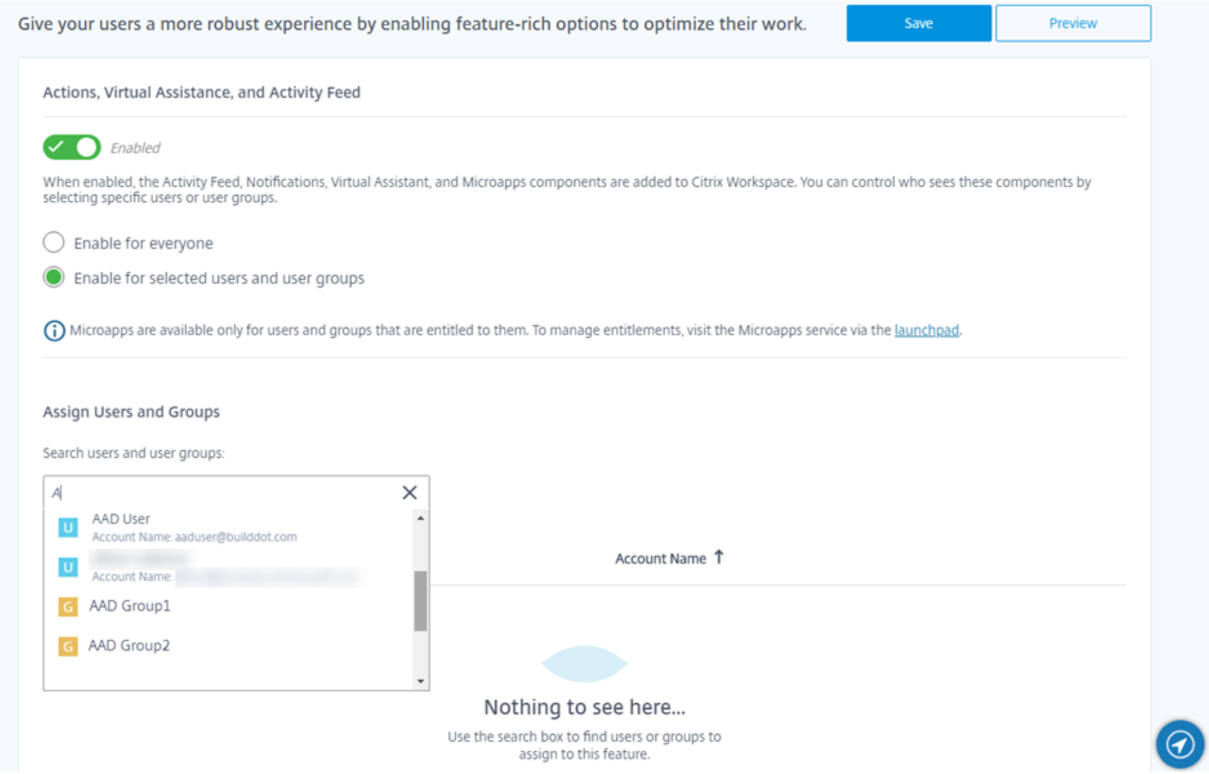
When enabled, the following components are added to Citrix Workspace: Activity Feed, Notifications, Virtual Assistant and Microapps (if activated). You can control who sees these components by selecting specific users or user groups.

ⓘ Microapps are available only for users and groups that are entitled to them. To manage entitlements, visit the Microapps service.

● 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 who will see the activity feed in their workspace. When you're finished adding users and groups, click **Save**.



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

Actions, Virtual Assistance, and Activity Feed

Enabled

When enabled, the Activity Feed, Notifications, Virtual Assistant, 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

ⓘ 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

Search users and user groups:

A

U AAD User
Account Name: aaduser@builddot.com

U [redacted]
Account Name: [redacted]

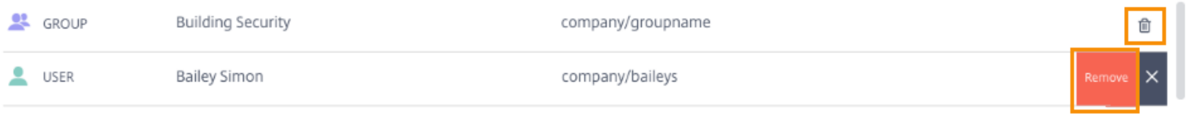
G AAD Group1

G AAD Group2

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**, click the trash can icon for the user or group and then select **Remove**.



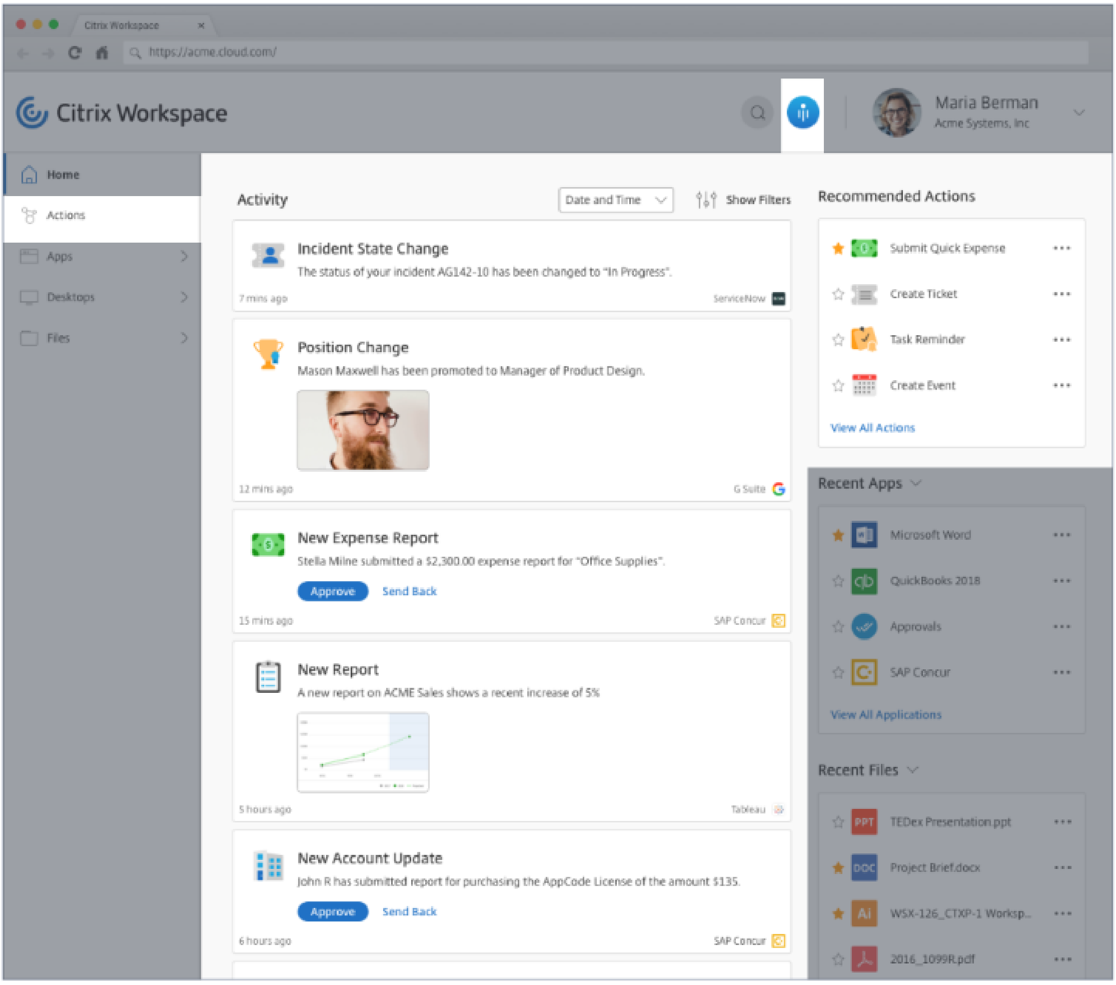
GROUP	Building Security	company/groupname	
USER	Bailey Simon	company/baileys	Remove

Preview the workspace

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

Subscriber experience with Actions, Virtual Assistance, and Activity Feed

When enabled, subscribers see personalized alerts and notifications in their **Activity** feed, in the center of their workspace. At the top of the workspace, the blue **Citrix Assistant** icon appears.



Incident State Change
The status of your incident AG142-10 has been changed to "In Progress".
7 mins ago — ServiceNow

Position Change
Mason Maxwell has been promoted to Manager of Product Design.
12 mins ago — G Suite

New Expense Report
Stella Milne submitted a $2,300.00 expense report for "Office Supplies".
Approve — Send Back
15 mins ago — SAP Concur

New Report
A new report on ACME Sales shows a recent increase of 5%
5 hours ago — Tableau

New Account Update
John R has submitted report for purchasing the AppCode License of the amount $135.
Approve — Send Back
6 hours ago — SAP Concur

If the subscriber needs to take action on an item, such as approving a request, they can take that action directly in the activity feed. They don't have to switch to another application to complete actions.

Recommended 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 then processed by your organizational systems through the integrations you've created in the Microapps service.

The **Actions** tab on the left side 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.

To use Citrix Assistant, subscribers click the blue **Citrix Assistant** icon at the top of the workspace. Subscribers can then type their query and view the response within their workspace. The queries that Citrix Assistant can process depend on the resolvers that you've configured in the Microapps service. For more information, see Configure Citrix Assistant resolvers.

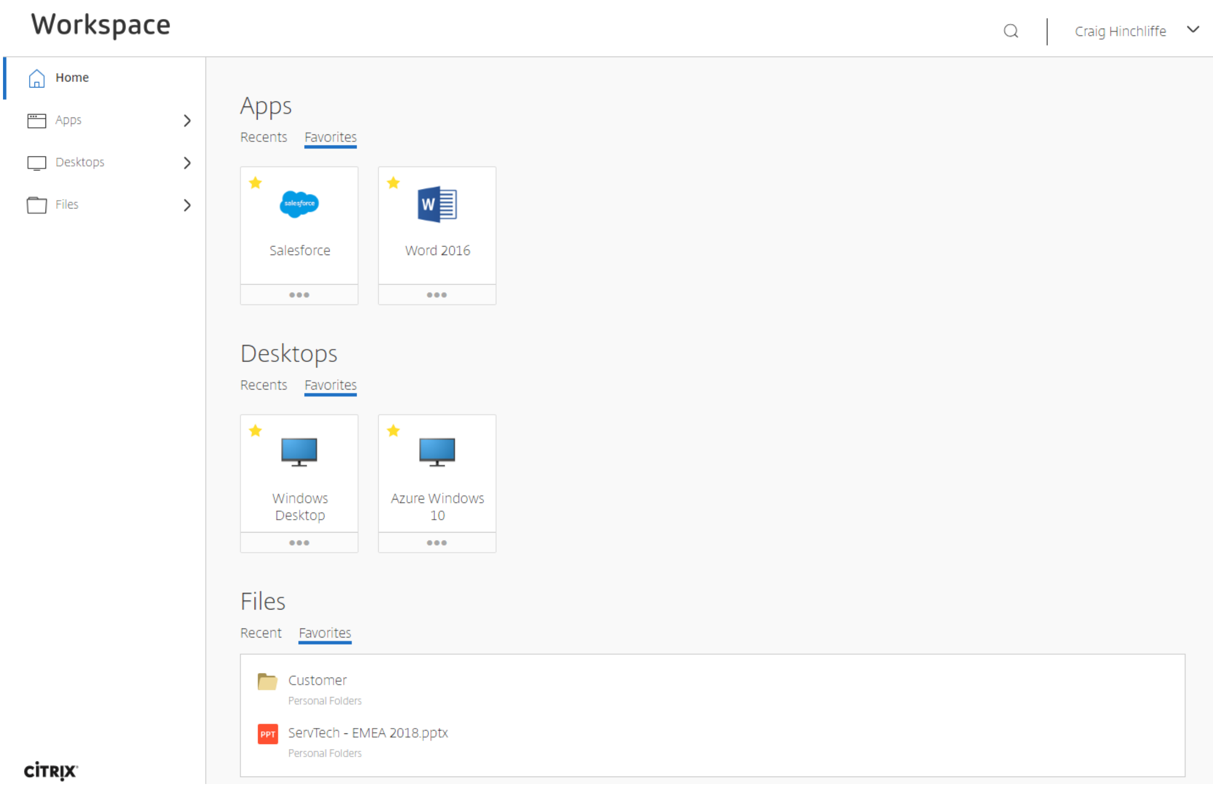
Customize workspace preferences

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

Allow Favorites

Allow Favorites is available to customers who have access to Workspace Configuration and the new workspace experience.

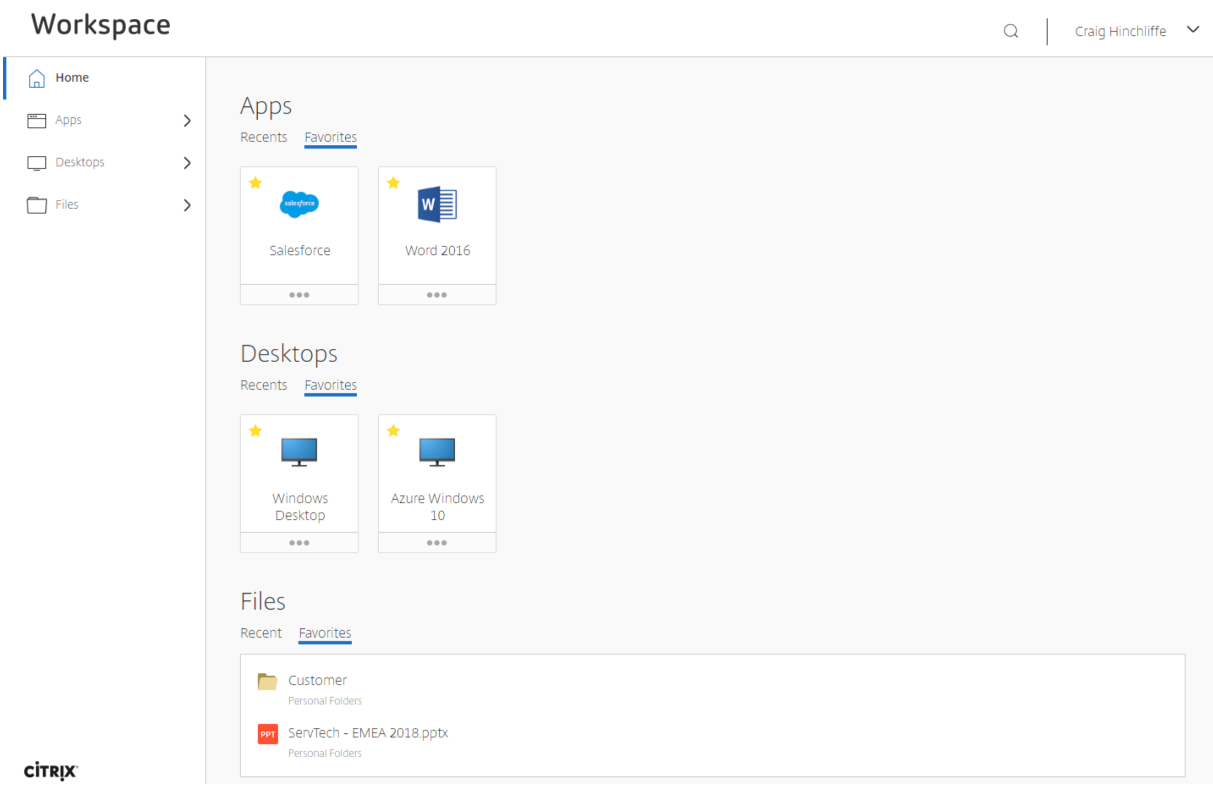
Enabled (default). Workspace subscribers can add favorite apps (up to a maximum of 250) by selecting the star icon.



Disabled. Subscribers can't select apps as favorites. Favorites are not deleted and can be recovered if you re-enable Favorites.

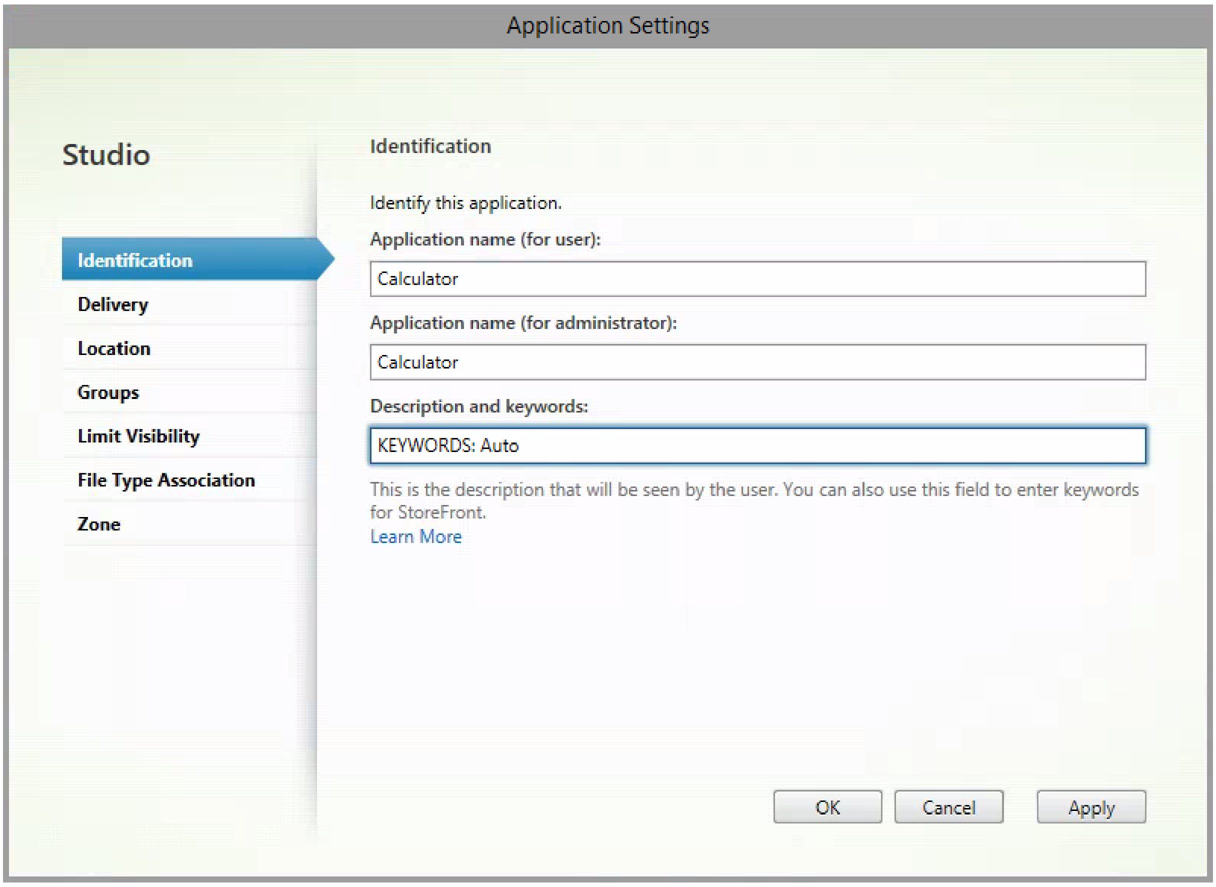
> **Note:**
>
> For some existing customers (new to workspace between December 2017 and April 2018), **Allow Favorites** defaults to **Disabled**. The administrator can decide when to enable this feature for their subscribers.

Subscribers can add up to a maximum of 250 favorite apps. If a subscriber adds more than 250, the "oldest favorite" app will be removed (or as close as possible to preserve the most recent favorites).



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**).

- **KEYWORDS: Auto**. The application is added as a favorite, however subscribers can remove the favorite.
- **KEYWORDS: Mandatory**. The application is added as a favorite, however subscribers cannot remove the favorite. Mandatory apps do not display a star icon.



Application Settings

Studio

Identification

Identify this application.

Application name (for user): Calculator

Application name (for administrator): Calculator

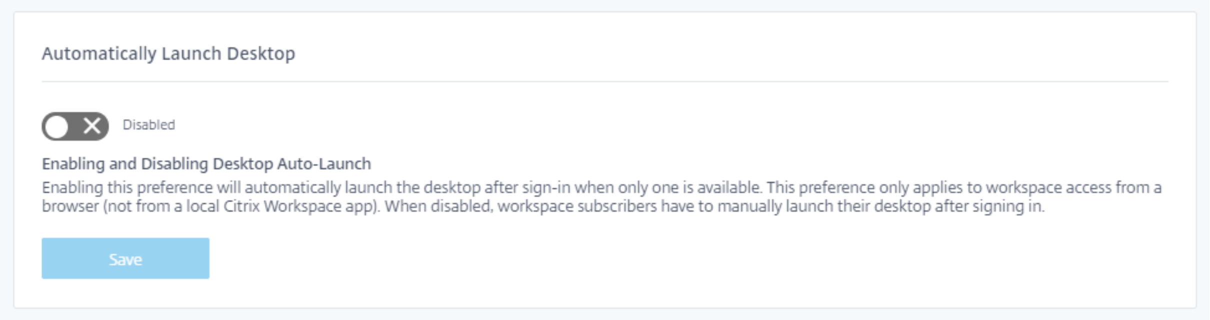
Description and keywords: KEYWORDS: Auto

This is the description that will be seen by the user. You can also use this field to enter keywords for StoreFront.

Learn More

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.



Automatically Launch Desktop

Disabled

Enabling and Disabling Desktop Auto-Launch

Enabling this preference will automatically launch the desktop after sign-in when only one is available. This preference only applies to workspace access from a browser (not from a local Citrix Workspace app). When disabled, workspace subscribers have to manually launch their desktop after signing in.

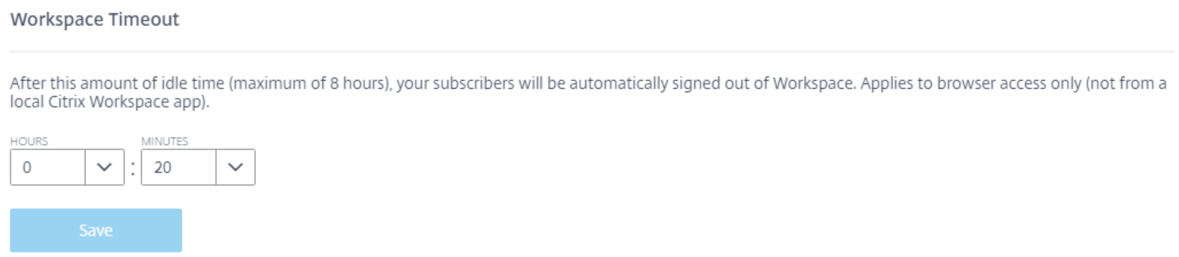
When disabled (default), the setting prevents Citrix Workspace from automatically starting a desktop when a subscriber signs in. Subscribers must manually launch their desktop after signing in.

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.

Workspace Timeout

Use the Workspace Timeout preference to specify the amount of idle time allowed (up to a maximum of 8 hours) before subscribers are automatically signed out of Citrix Workspace. This preference applies to browser access only, and does not apply to access from a local Citrix Workspace app.



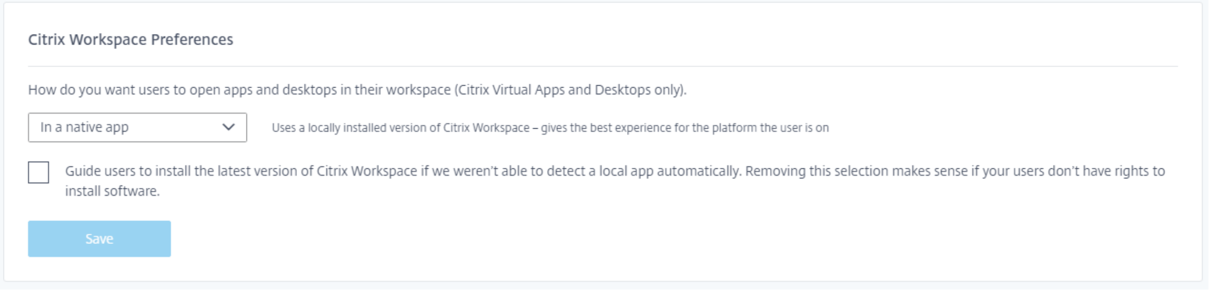
Workspace Timeout

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 0 : MINUTES 20

Citrix Workspace Preferences

Citrix Workspace Preferences 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 does not apply to, for example, SaaS apps delivered by the Citrix Gateway service. This preference is available to new and existing customers, however the introduction of this feature will not change any settings for existing customers.



Citrix Workspace Preferences

How do you want users to open apps and desktops in their workspace (Citrix Virtual Apps and Desktops only).

In a native app — Uses a locally installed version of Citrix Workspace – gives the best experience for the platform the user is on

□ 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.

Choose one of the following settings:

- **In a native app** (default). Uses a locally installed version of Citrix Workspace – gives the best experience for the platform the user is on.
- **In a browser**. Uses Citrix Workspace for HTML5 – no client software is required.

- **Let users choose**. Prompts users to detect a locally installed version of Citrix Workspace, or to use Citrix Workspace for HTML5 in their browser where possible.

For the **In a native app** and **Let users choose** options, there is an additional check box option to guide users to install the latest version of Citrix Workspace if a local app can't be detected automatically. Removing this selection makes sense if your users don't have rights to install software.

Copied!
Failed!

Aggregate on-premises virtual apps and desktops in workspaces

May 27, 2020

If you have an on-premises Virtual Apps and Desktops deployment, you can add your Site to Citrix Workspace to make your existing on-premises apps and desktops available to workspace 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.

Watch this video to learn more about how you can integrate your on-premises apps and desktops into subscribers' workspaces:

> **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 are not supported for use with Citrix Workspace.

> **Important:**
>
> XenApp and XenDesktop 7.x includes versions which are End of Life. XenApp and XenDesktop Current Releases prior to 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 is conditional upon successful enumeration and launch of resources with your existing StoreFront on-premises deployment.
>
> XenApp 6.5 reached End of Life on June 30, 2018. Support for Workspace Site aggregation with End of Life versions of XenApp is conditional on the successful enumeration and launch of resources in your existing 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 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 be able to 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.
- Does not have any other Citrix components installed, is not an Active Directory domain controller, and is not 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 need to 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 Internet 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.

Although you can install the Cloud Connectors during the process of your adding your Site to Citrix Workspace, Citrix recommends installing them beforehand to ensure your Site is added with minimal interruption.

Web proxy configuration

If you have a web proxy in your environment, you must ensure 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. Do not 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 will be 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 cannot use separate user and resource forests when you define the default resource location during the process of adding your Site. Because the Cloud Connectors do not 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 are not supported for Site aggregation. Although Citrix Cloud and Citrix Workspace support users from untrusted forests, these users are not able to use Citrix Workspace after an on-premises Site has been 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 you make 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 their 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 have 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 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 does not 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. 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 are not 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 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 the 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 re-order 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 located 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 are 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, but 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 does not make any changes to your Site.

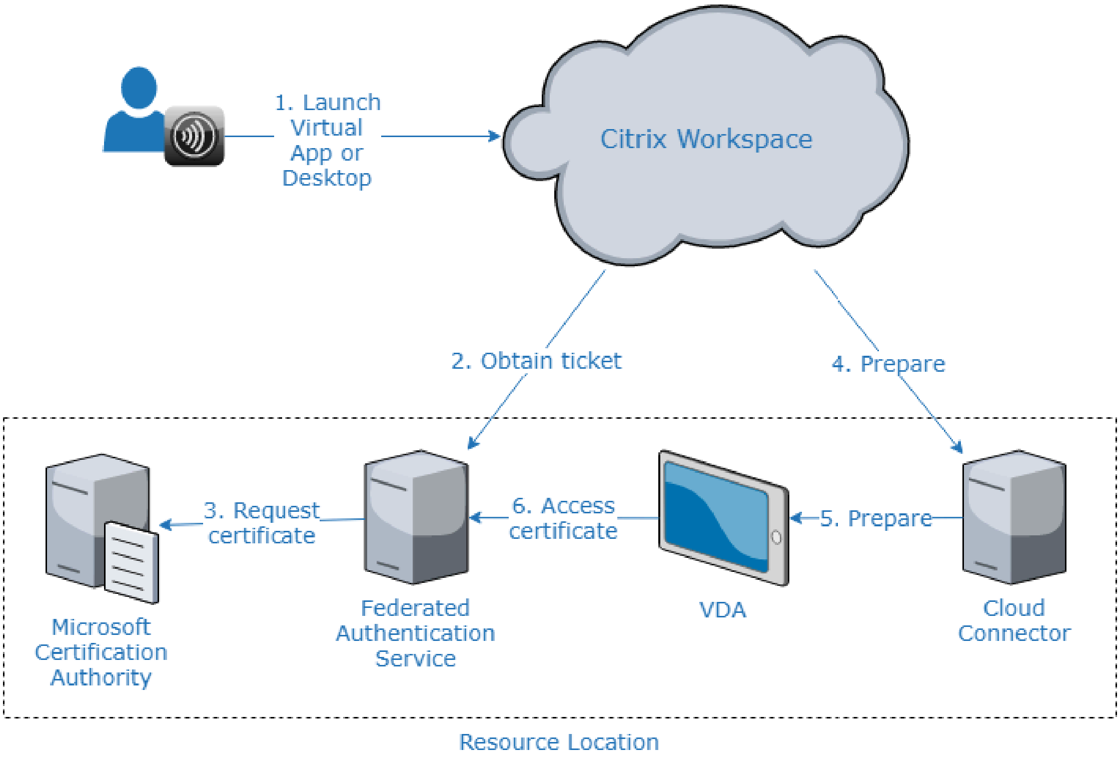
1. On the **Sites** page, click the ellipsis button for the Site you want to remove.
2. Click **Delete**.

Copied!
Failed!

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

July 7, 2020

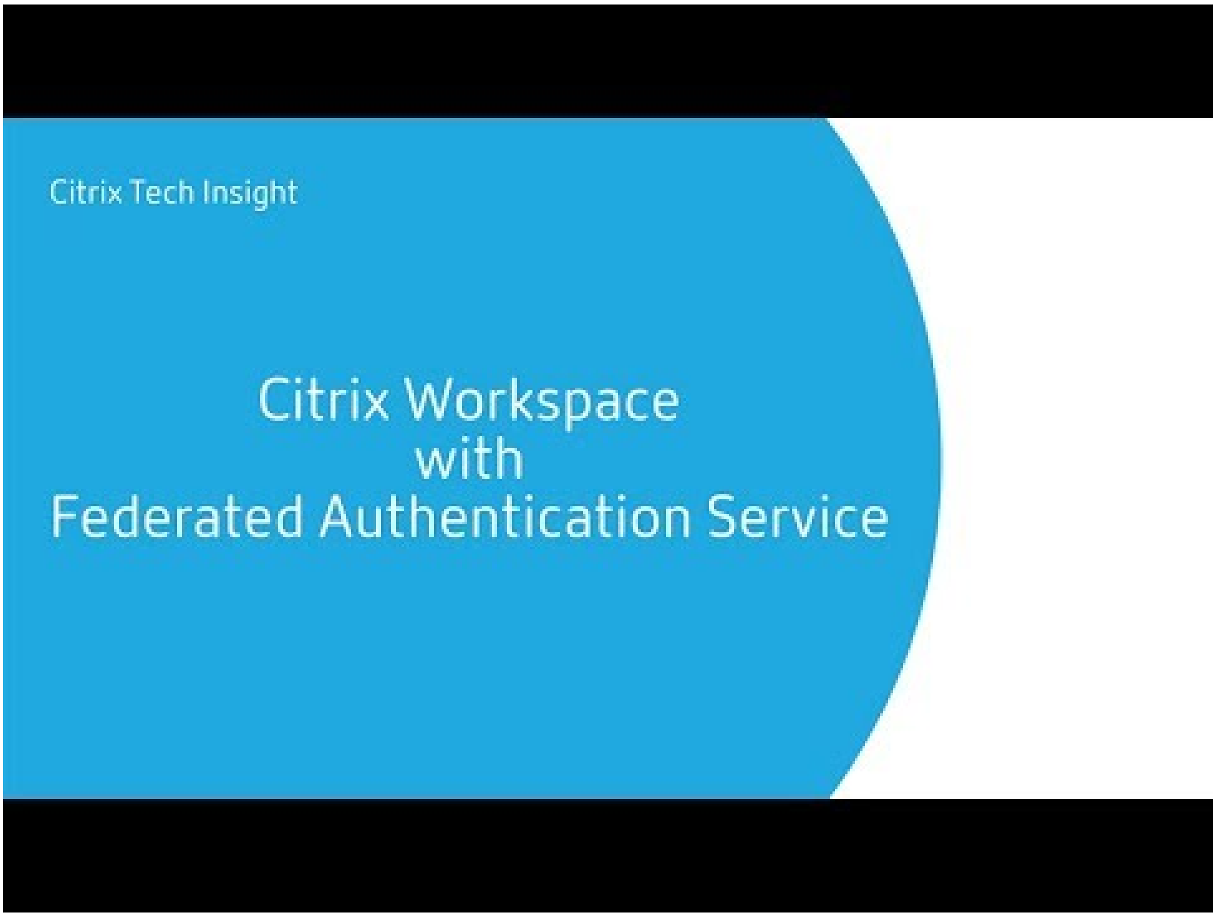
Citrix Federated Authentication Service (FAS) supports single sign-on to virtual apps and desktops in Citrix Workspace. Within each resource location, you can connect multiple FAS servers to Citrix Cloud for load balancing and failover purposes. You can use the same FAS server for both on-premises and Citrix Cloud with proper rule configuration.



Subscribers signing in to their workspaces through Azure AD enter their credentials only once to access their apps and desktops. When subscribers launch a virtual app or desktop in their workspace, Citrix Cloud selects a FAS server in the same resource location as the VDA 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 FAS and presents the ticket.

> **Important:**
>
> - When you enable single sign-on through FAS, single sign-on is active only in the resource locations where you have connected FAS servers. If there are no FAS servers in a resource location, single sign-on is not active for resources in that resource location.
> - When you enable FAS in your resource location, the Federated Authentication Service is active for all virtual app and desktop launches from Citrix Workspace.

For an overview of the Federated Authentication Service for Citrix Workspace, view this Tech Insight video:



Requirements

Connectivity requirements

Connecting a FAS server to Citrix Cloud is performed using the FAS administration console. This console can be used to configure a local or remote FAS server. For this feature to function, the console and FAS service access the following addresses using the user's account and the Network Service account, respectively.

- FAS administration console, under the user's account
  - `*.cloud.com`
  - `*.citrixworkspaceapi.net`
  - Addresses required by a third party identity provider, if one is used in your environment
- FAS service, under the Network Service account: `*.citrixworkspaceapi.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 server

For complete requirements for the FAS server, see the System Requirements section of the FAS product documentation.

If you don't already have a FAS server in your on-premises Virtual Apps and Desktops environment or you want to upgrade an existing FAS server, see Install and configure FAS in this article.

If your existing FAS server is Version 10.0 or later, proceed to Connect a FAS server to Citrix Cloud.

Citrix Workspace

You must have the 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 Connector enables communication between your resource location (where the FAS server resides) and Citrix Cloud. You need at least two servers on which to install the Cloud Connector software to ensure high availability. These servers must meet the following requirements:

- Meets the system requirements described in Cloud Connector Technical Details
- Has no other Citrix components installed, is not an Active Directory domain controller, and is not a machine critical to your resource location infrastructure.
- Joined to the domain where your FAS server resides.

For more information about deploying Cloud Connectors, refer to the following articles:

- Cloud Connector Proxy and Firewall Configuration
- Cloud Connector Installation

Install and configure FAS

Install and configure one or more FAS servers if:

- You don't already have a FAS server in your on-premises environment.
- Your existing FAS server is older than Version 10.0 and you want to upgrade it in-place so you can connect to Citrix Cloud.

If your existing FAS server is Version 10.0 or later, proceed to Connect a FAS server to Citrix Cloud.

> **Important:**
>
> When you enable single sign-on through FAS, single sign-on is active only in the resource locations where you have connected FAS servers. If there are no FAS servers in a resource location, single sign-on is not active for workspace subscribers connecting through that resource location.

Guidance for installing and configuring FAS

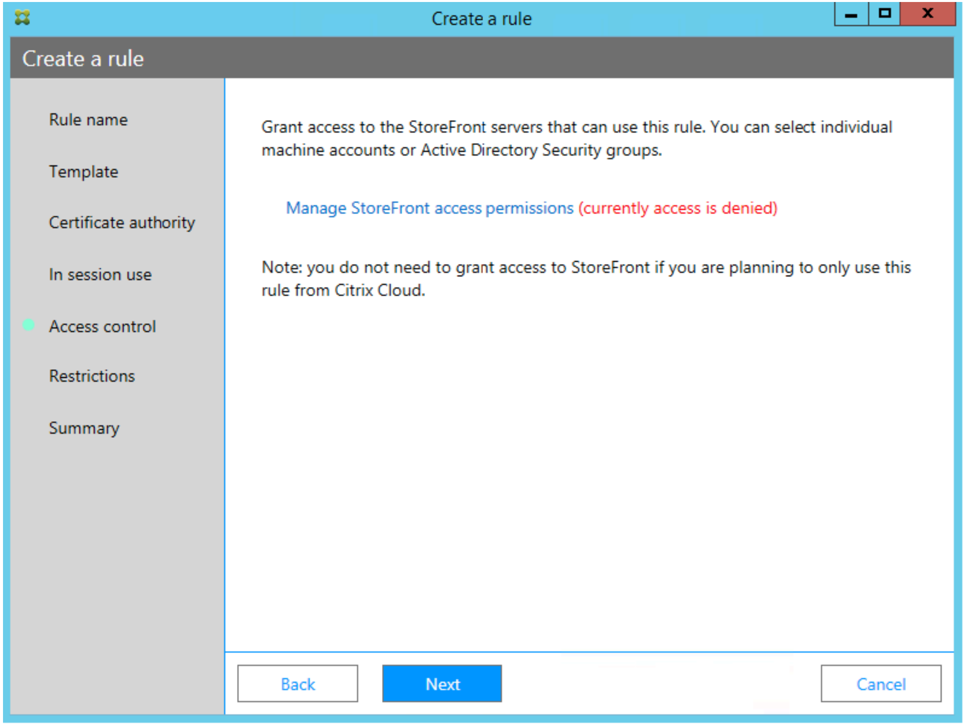
Installing and configuring a FAS server follows the same process as described in the FAS documentation, with the following exceptions:

- Configuration steps for StoreFront or the Delivery Controller are not required.
- The FAS administration console might look different to the FAS product documentation. However, the functionality is the same.
- The FAS administration console does not require you to specify which FAS server you want to connect. It connects to the local FAS service by default. If needed, you can connect to a remote service using **Connect to another server** in the top right of the console.

To install and configure a FAS server, you perform the following tasks:

1. Download and install the latest version of the FAS server software from Citrix.

2. Configure FAS rules.



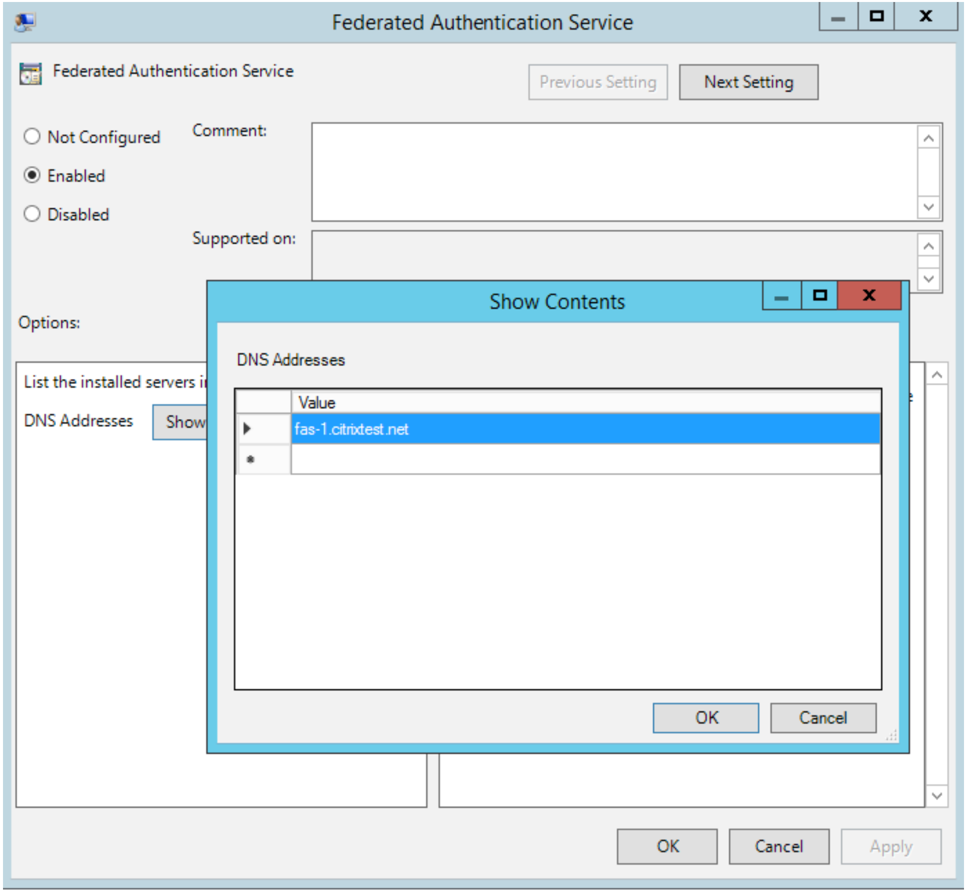
Grant access to the StoreFront servers that can use this rule. You can select individual machine accounts or Active Directory Security groups.

Manage StoreFront access permissions (currently access is denied)

Note: you do not need to grant access to StoreFront if you are planning to only use this rule from Citrix Cloud.

When you configure a FAS rule, you can specify which StoreFront servers are allowed to use the rule. However, when a rule is used with Citrix Cloud, the StoreFront access permissions are ignored. You can use the same rule with Citrix Cloud and with an on-premises StoreFront deployment. StoreFront access permissions are still applied when the rule is used by an on-premises StoreFront. If you are using the FAS server only with Citrix Cloud, you don't have to perform this task.

3. Configure Group Policy even if you are using your FAS deployment with Citrix Cloud only.



○ Not Configured
● Enabled
○ Disabled

DNS Addresses

	Value
▶	fas-1.citrixtest.net
*	

The order of DNS addresses of your FAS servers in the list must be consistent as seen by:

- VDAs
- StoreFront servers (if present)
- FAS servers

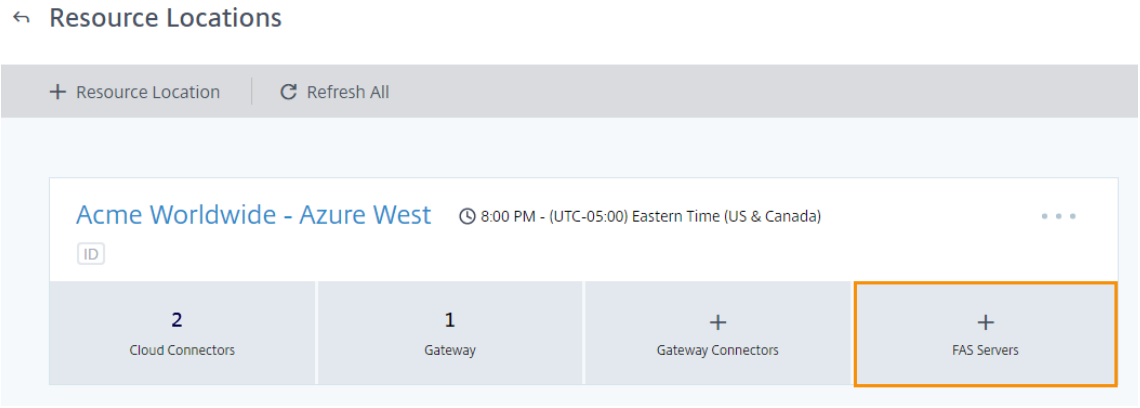
This is because an index (integer) into the list is used by the VDA to locate the FAS server chosen for a virtual app or desktop launch.

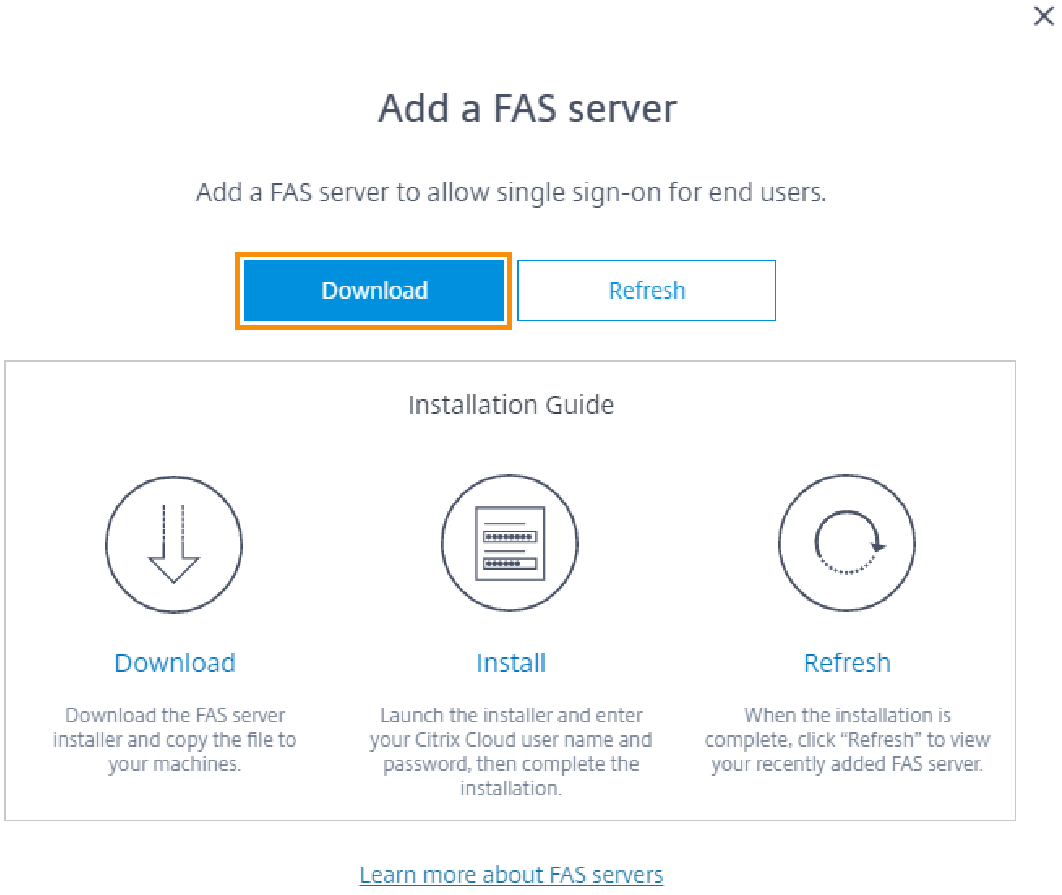
Download the FAS software

The latest version of the FAS sofware is available from the Citrix Downloads web site at https://www.citrix.com/down cloud/betas-and-tech-previews/federated-authentication-service–fas-.html.

To access the Federated Authentication Service downloads page from within the Citrix Cloud console:

1. From the Citrix Cloud menu, select **Resource Locations**.
2. Select the **FAS Servers** tile and then click **Download**.




Add a FAS server

Add a FAS server to allow single sign-on for end users.

Download

Download the FAS server installer and copy the file to your machines.

Install

Launch the installer and enter your Citrix Cloud user name and password, then complete the installation.

Refresh

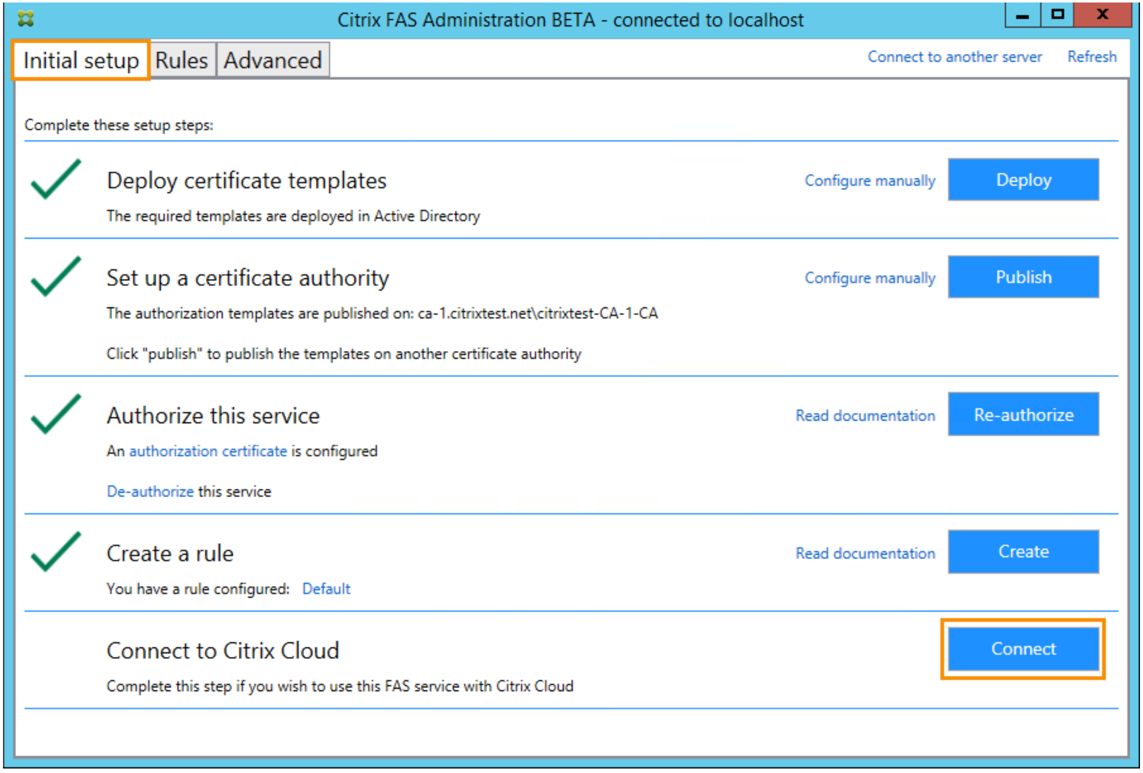
When the installation is complete, click "Refresh" to view your recently added FAS server.

After downloading, you can launch the installer and follow the wizard to configure FAS rules and group policies and connect to Citrix Cloud.

Connect a FAS server to Citrix Cloud

This section assumes your existing FAS server is installed and configured as described in the FAS documentation.

1. From the FAS installer, ensure the **Initial Setup** tab is selected.



Citrix FAS Administration BETA - connected to localhost

Complete these setup steps:

✓ Deploy certificate templates

The required templates are deployed in Active Directory

✓ Set up a certificate authority

The authorization templates are published on: ca-1.citrixtest.net\citrixtest-CA-1-CA

Click "publish" to publish the templates on another certificate authority

✓ Authorize this service

An authorization certificate is configured

De-authorize this service

✓ Create a rule

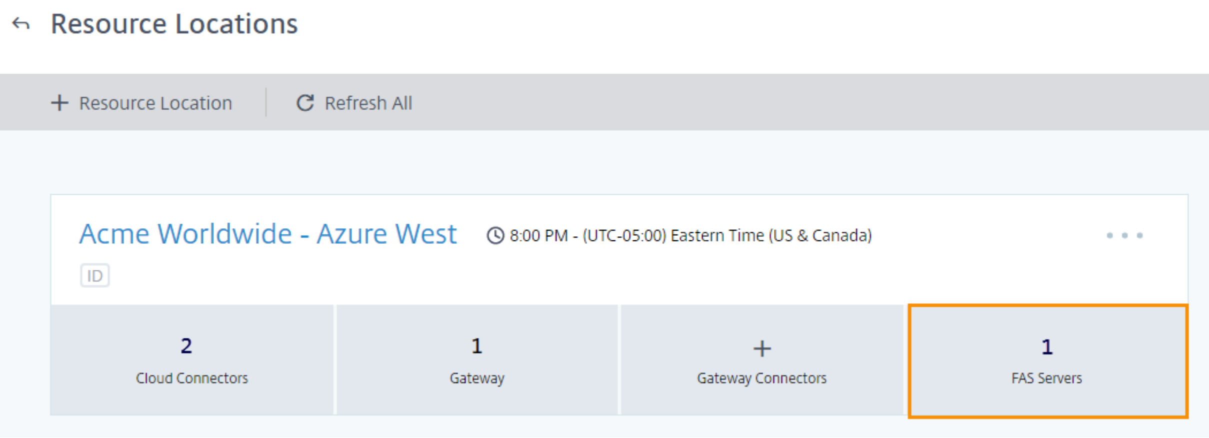
You have a rule configured: Default

Connect to Citrix Cloud

Complete this step if you wish to use this FAS service with Citrix Cloud

2. In **Connect to Citrix Cloud**, select **Connect**.
3. When prompted, sign in to Citrix Cloud, select the customer account, if applicable, and select the resource location where you want to connect the FAS server.

After you complete the installation, Citrix Cloud registers the FAS server and displays it on the Resource Locations page in your Citrix Cloud account.



Resource Locations

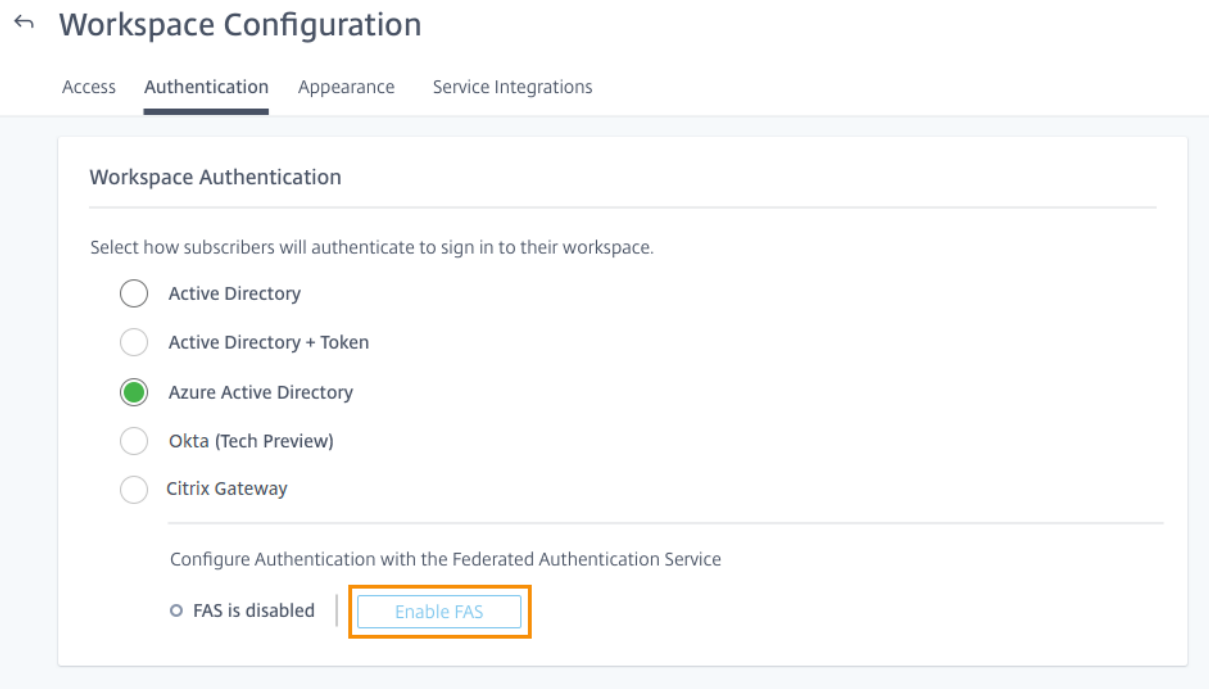
Acme Worldwide - Azure West

8:00 PM - (UTC-05:00) Eastern Time (US & Canada)

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

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.



Workspace Configuration

Workspace Authentication

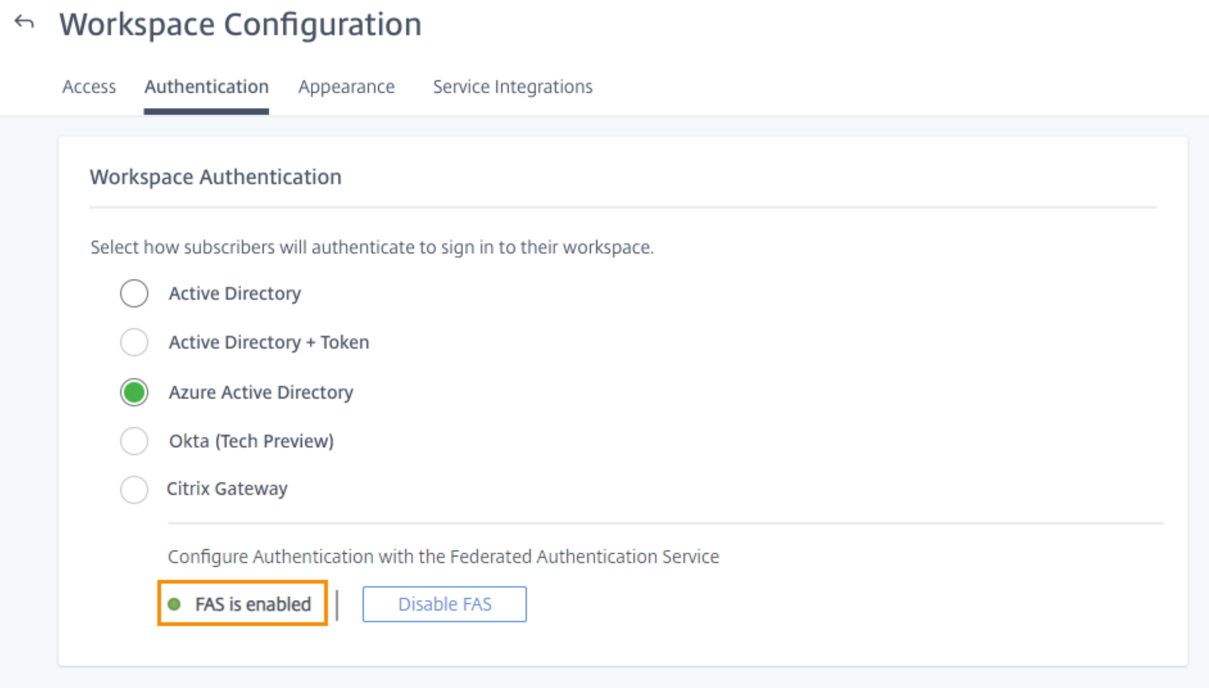
Select how subscribers will authenticate to sign in to their workspace.

○ Active Directory
○ Active Directory + Token
● Azure Active Directory
○ Okta (Tech Preview)
○ Citrix Gateway

Configure Authentication with the Federated Authentication Service

○ FAS is disabled

Afterward, the Federated Authentication Service is active for all virtual app and desktop launches from Citrix Workspace.



Workspace Authentication

Select how subscribers will authenticate to sign in to their workspace.

- ○ Active Directory
- ○ Active Directory + Token
- ● Azure Active Directory
- ○ Okta (Tech Preview)
- ○ Citrix Gateway

Configure Authentication with the Federated Authentication Service

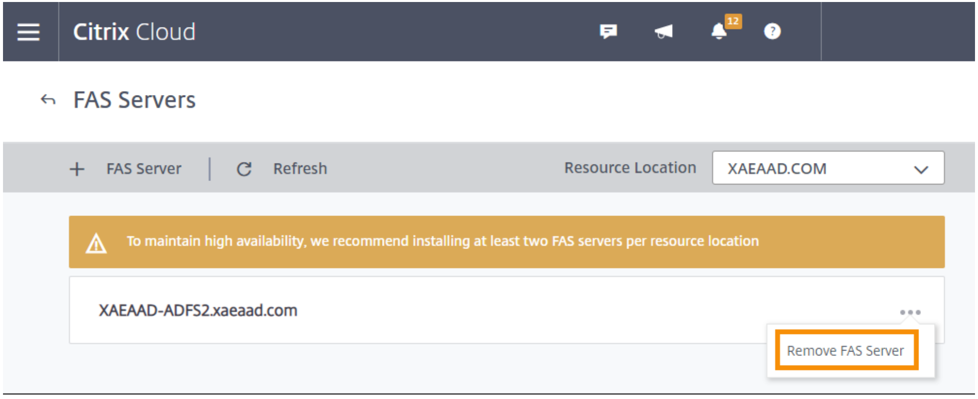
FAS is enabled | Disable FAS

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 a FAS server is 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

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 button, and then select **Remove FAS Server**.



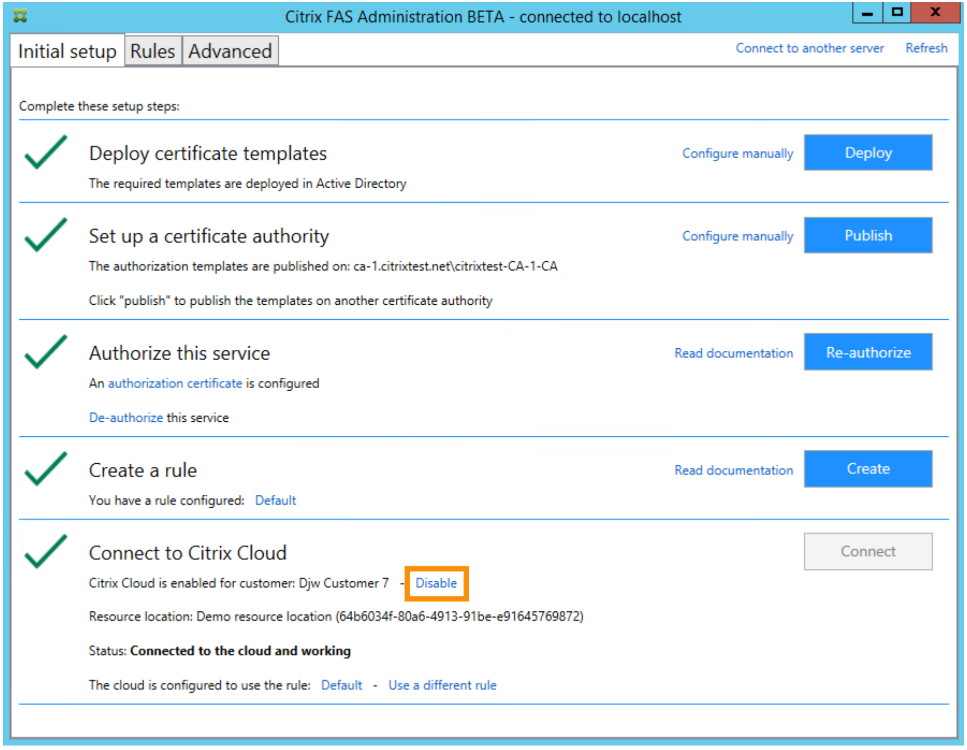
Resource Location: XAEAAD.COM

To maintain high availability, we recommend installing at least two FAS servers per resource location

XAEAAD-ADFS2.xaeaad.com

Remove FAS Server

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



Complete these setup steps:

✓ Deploy certificate templates

The required templates are deployed in Active Directory

✓ Set up a certificate authority

The authorization templates are published on: ca-1.citrixtest.net\citrixtest-CA-1-CA

Click "publish" to publish the templates on another certificate authority

✓ Authorize this service

An authorization certificate is configured

De-authorize this service

✓ Create a rule

You have a rule configured: Default

✓ Connect to Citrix Cloud

Citrix Cloud is enabled for customer: Djw Customer 7 - Disable

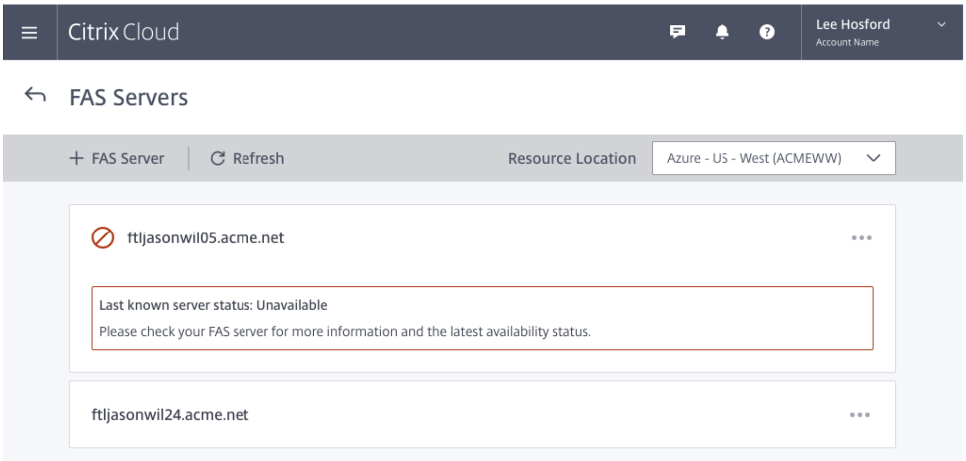
Resource location: Demo resource location (64b6034f-80a6-4913-91be-e91645769872)

Status: **Connected to the cloud and working**

The cloud is configured to use the rule: Default - Use a different rule

Troubleshooting

If the FAS server is not available, a warning message appears on the FAS Servers page.



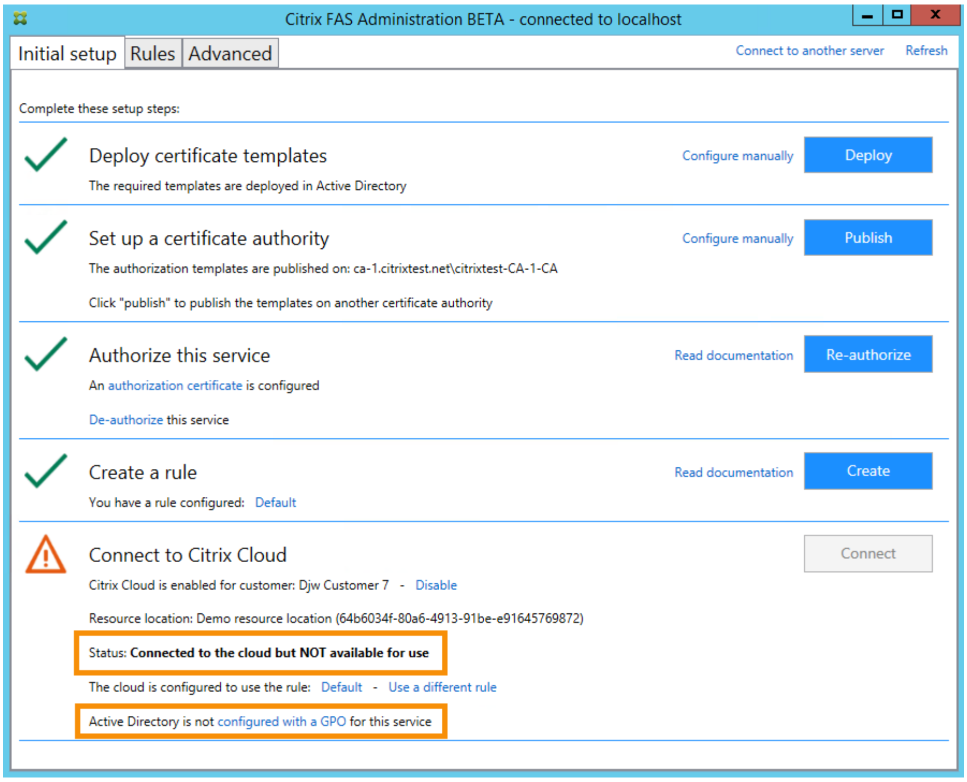
ftljasonwil05.acme.net

Last known server status: Unavailable

Please check your FAS server for more information and the latest availability status.

ftljasonwil24.acme.net

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:



Complete these setup steps:

✓ Deploy certificate templates

The required templates are deployed in Active Directory

✓ Set up a certificate authority

The authorization templates are published on: ca-1.citrixtest.net\citrixtest-CA-1-CA

Click "publish" to publish the templates on another certificate authority

✓ Authorize this service

An authorization certificate is configured

De-authorize this service

✓ Create a rule

You have a rule configured: Default

⚠ Connect to Citrix Cloud

Citrix Cloud is enabled for customer: Djw Customer 7 - Disable

Resource location: Demo resource location (64b6034f-80a6-4913-91be-e91645769872)

Status: **Connected to the cloud but NOT available for use**

The cloud is configured to use the rule: Default - Use a different rule

Active Directory is not configured with a GPO for this service

If the FAS Administration console indicates that the server is operating properly, but there are still VDA logon problems, consult the FAS Troubleshooting Guide.

Additional help and support

For troubleshooting help, questions, or to provide feedback about federated authentication for workspaces, visit the Federated Authentication Service for Workspace Preview support forum to talk with Citrix experts and other members of the Citrix Cloud community.

Copied!
Failed!

Optimize connectivity to workspaces with Direct Workload Connection

June 29, 2020

> **Note:**
>
> This feature is currently in Limited Release. The feature can be used in a production environment, but might not be suitable for all customers. For more information, refer to the About this Limited

> Release in this article.

With Direct Workload Connection in Citrix Cloud, you can optimize internal traffic to the apps and desktops you make available to subscribers' workspaces to make HDX sessions faster. Ordinarily, users on both internal and external networks have to connect to VDAs through an external gateway. While this is expected for external users, internal users experience slower connections to virtual resources. 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 configure network locations that correspond to the VDAs in your environment with the Network Location Service. To configure these locations, you use a PowerShell module that Citrix provides. These network locations correspond to the public IP ranges of the networks where your internal users will be connecting from (for example, your office or branch locations). When subscribers launch Virtual Apps and Desktops sessions from their workspace, Citrix Cloud detects whether subscribers are internal or external to the company network based on the public IP address of the network from which they're connecting. 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 the subscriber through Citrix Gateway as expected and then redirects the subscriber through the Citrix Cloud Connector to the VDA in the internal network.

About this Limited Release

The Network Location Service (NLS), which Direct Workload Connection uses, is currently hosted in multiple availability zones in Amazon Web Service's US-East region. A call to the NLS is made at desktop or app launch time in parallel with many other calls. NLS checks the public IP address that the call came from and responds with whether the user is internal or external. In the rare case that a response isn't received from NLS before the other parallel calls return, the launch is routed through the Gateway.

The NLS is hosted in a single PoP. So, if AWS has a region-wide outage in the US-East region that affected all availability zones, the NLS goes offline. To date, AWS has never suffered a region-wide outage and has a 99.999% uptime guarantee. However, if an outage occurs, all launches are routed through the Gateway instead of directly to the VDAs. Launches are routed through VDAs when the US-East region is online again. Although no launch failures or delays would occur, latency would revert to the levels you previously experienced before enabling Direct Workload Connection. Citrix recommends that you consider whether you can accept this possibility before enabling Direct Workload Connection.

Supported products

Direct Workload Connection is supported for the Virtual Apps and Desktops service only. Support for Citrix Managed Desktops and Citrix SD-WAN is in Limited Release.

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

Launches of Secure Browser, Citrix Virtual Apps Essentials, and Citrix Virtual Desktops Essentials are always routed through the gateway. So, these launches do not realize any performance improvements from configuring Direct Workload Connection.

Requirements

Network requirements

- If you have a corporate network and a guest Wifi network, these networks must have separate public IP addresses. If your corporate and guest networks share the same public IP address, users on the guest network can't launch Virtual Apps and Desktops sessions.
- You must use the public IP address ranges of the networks where your internal users will be connecting from. Internal users on these networks must have a direct connection to the VDAs. Otherwise, launches of virtual resources will fail as Workspace will attempt to route internal users directly to the VDA, which will not be 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 are 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 you have TLS enabled on the VDAs in your internal network to ensure direct connections to those VDAs. If VDAs don't have TLS enabled, app and desktop launches are routed through the Gateway when subscribers use Workspace app for HTML5. Launches using the desktop viewer are not affected. For more information about securing direct VDA connections with TLS, see CTX134123 in the Citrix Support Knowledge Center.

Configuration overview

To configure Direct Workload Connection, perform the following tasks:

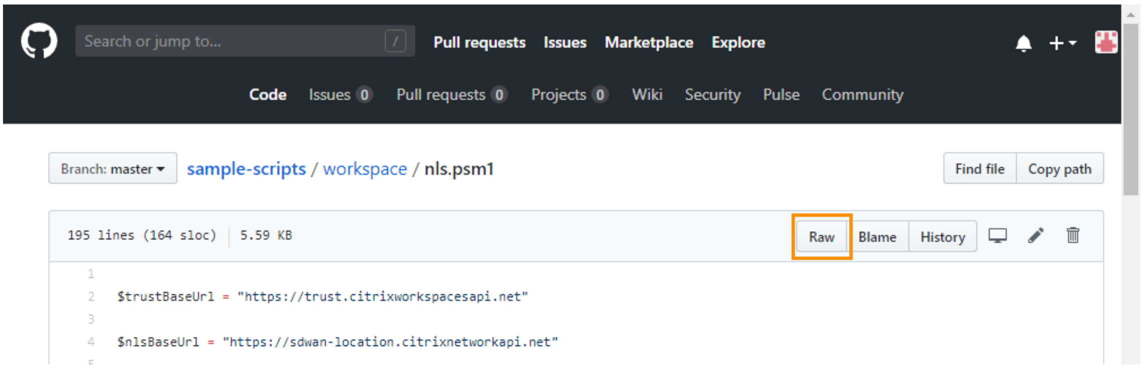
1. Determine the public IP address ranges of each branch location that your internal users will be connecting from.
2. Download the PowerShell module.
3. Create a secure API client in Citrix Cloud and make a note of the Client ID and secret.
4. Import the PowerShell module and connect to the Network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

Powershell module and configuration

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.



```
$trustBaseUrl = "https://trust.citrixworkspacesapi.net"

$nlsBaseUrl = "https://sdwan-location.citrixnetworkapi.net"
```

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

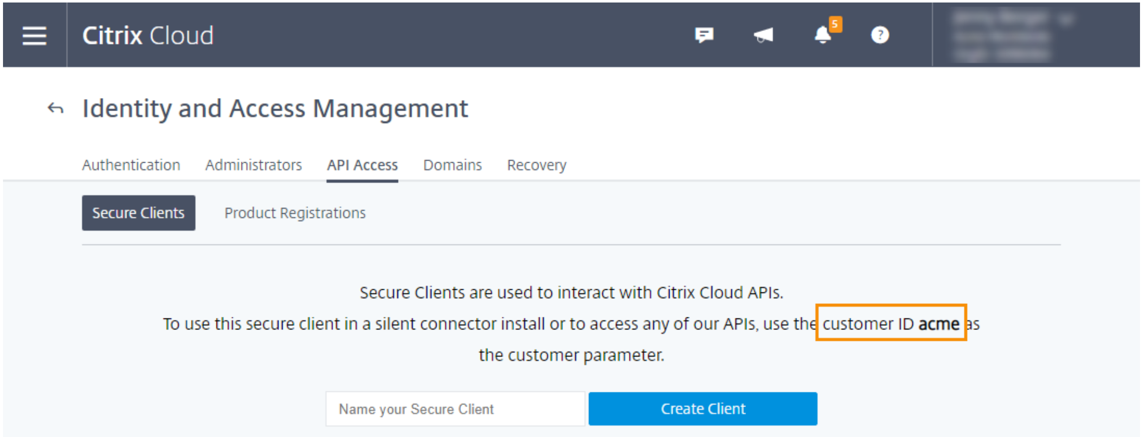
Required configuration details

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.

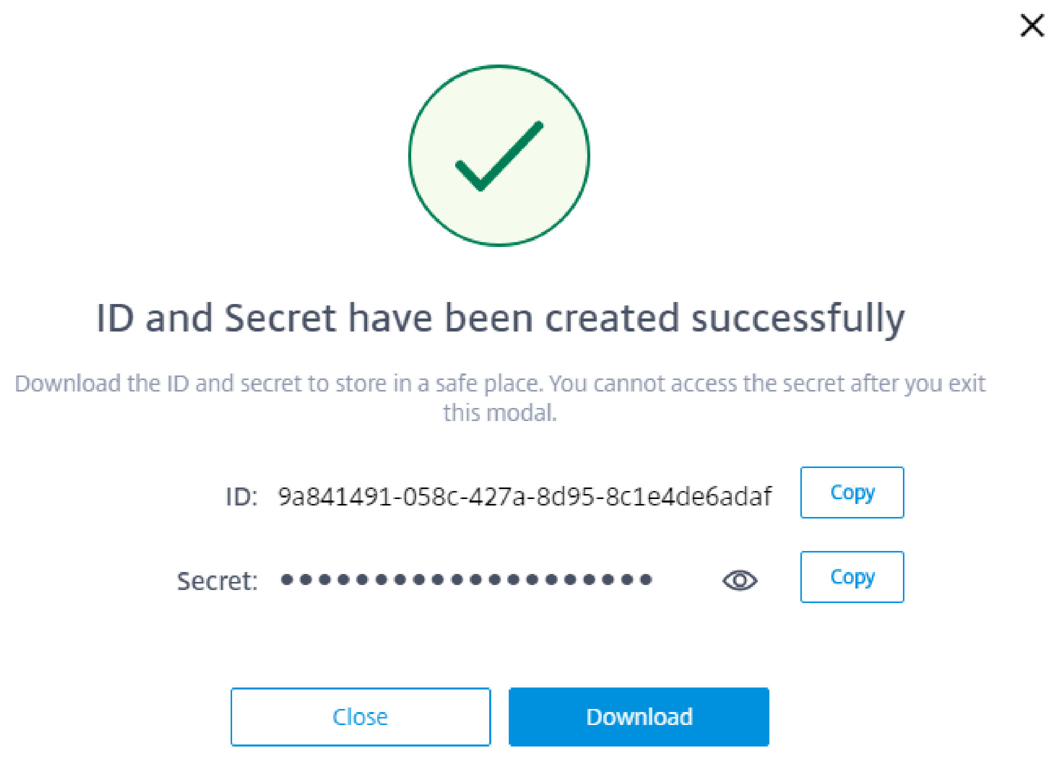
Create a secure client

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.



Secure Clients are used to interact with Citrix Cloud APIs.
To use this secure client in a silent connector install or to access any of our APIs, use the customer ID **acme** as the customer parameter.

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



ID and Secret have been created successfully

Download the ID and secret to store in a safe place. You cannot access the secret after you exit this modal.

ID: 9a841491-058c-427a-8d95-8c1e4de6adaf

Secret: ••••••••••••••••••••

Configure network locations

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

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

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

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

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 internal launches are routed correctly

To verify 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 **SSLProxyHost** 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

Use the steps in this section if you need to make changes to 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

Use the steps in this section if you need 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.

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

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

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

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

```

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

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

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

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

Troubleshooting

VDA launch failures

If VDA sessions are failing to launch, verify you 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.

Additional help and support

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

Copied!
Failed!

Secure workspaces

April 7, 2020

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

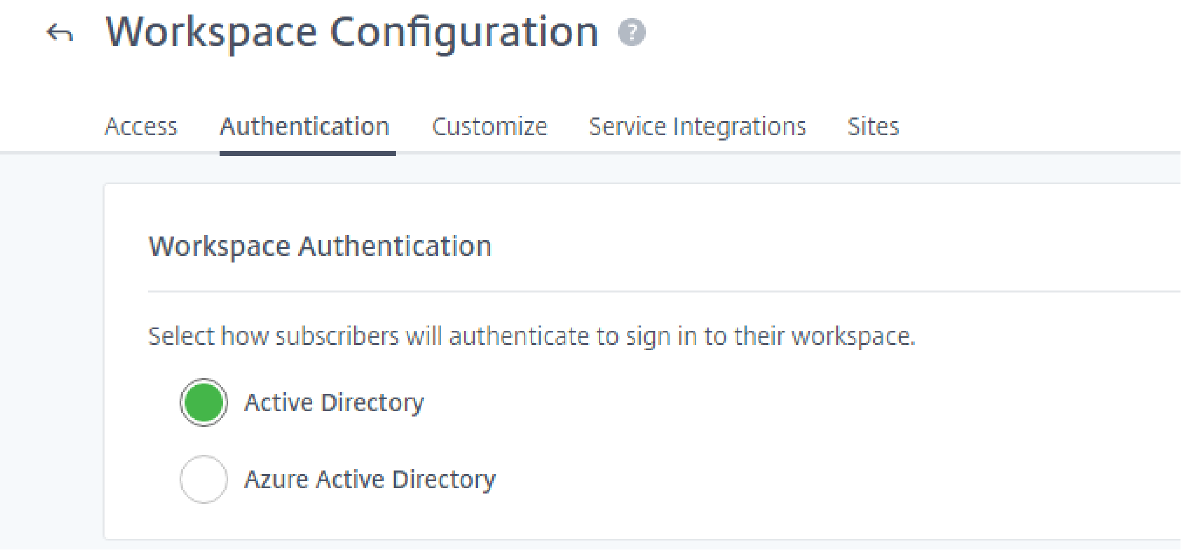
- Active Directory
- Active Directory plus token
- Azure Active Directory
- Citrix Gateway
- Okta

These authentication options are available to any Citrix Cloud service, including access control.

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

Change authentication methods

Change how subscribers authenticate to their workspace in **Workspace Configuration > Authentication > Workspace Authentication**.



Workspace Configuration

Workspace Authentication

Select how subscribers will authenticate to sign in to their workspace.

● Active Directory

○ Azure Active Directory

> **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.

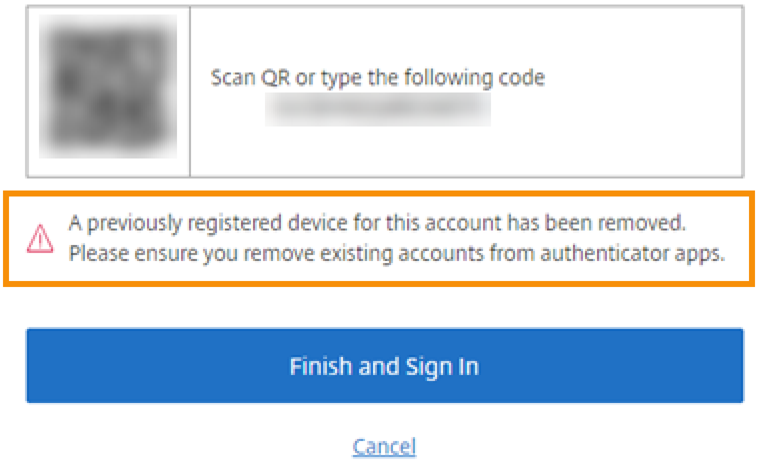
Active Directory plus token authentication has the following requirements:

- 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.

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:

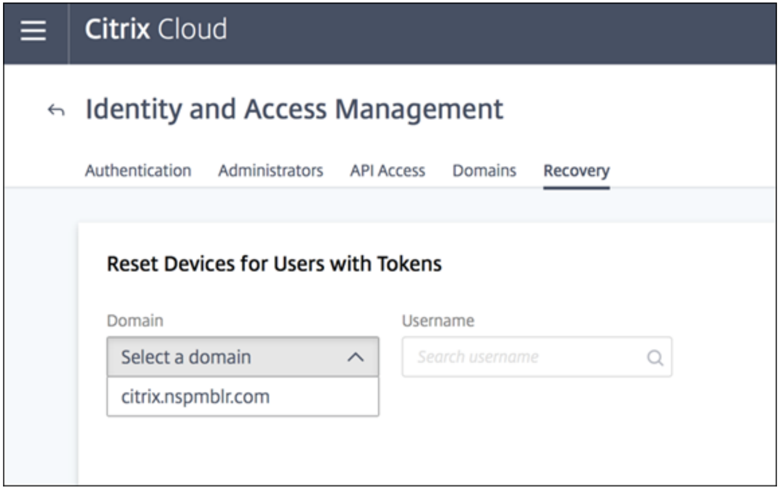
- Subscribers can re-enroll their devices using the same enrollment process described in Register devices for two-factor authentication. Because subscribers can enroll only one device at a time, enrolling a new device or re-enrolling an existing device removes the previous device registration.

  Scan QR or type the following code

  A previously registered device for this account has been removed. Please ensure you remove existing accounts from authenticator apps.

- 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.
- 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:

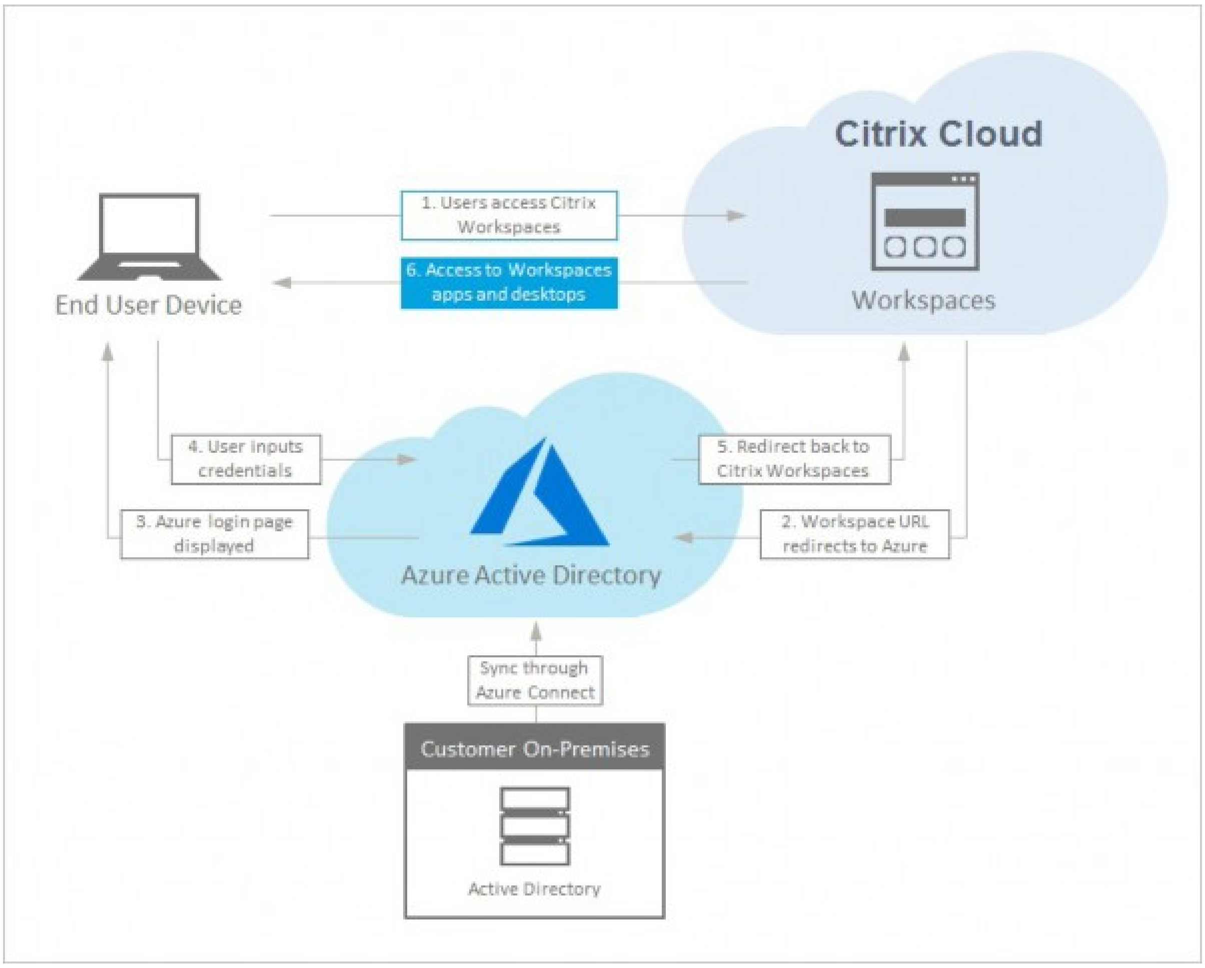
- **Manage users and user groups by using Citrix Cloud Library:** Use only the Citrix Cloud Library to manage users and user groups. (Do not specify users and user groups when creating or editing Delivery Groups.)

- **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 Cloud
Workspaces
End User Device
1. Users access Citrix Workspaces
6. Access to Workspaces apps and desktops
4. User inputs credentials
3. Azure login page displayed
5. Redirect back to Citrix Workspaces
2. Workspace URL redirects to Azure
Azure Active Directory
Sync through Azure Connect
Customer On-Premises
Active Directory

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 be-

tween 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.

Citrix Federated Authentication Service (Technical Preview)

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.

> **Note:**
>
> Using Federation Authentication Service with Citrix Cloud is currently in Technical Preview. Citrix recommends using technical preview features only in test environments.

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.

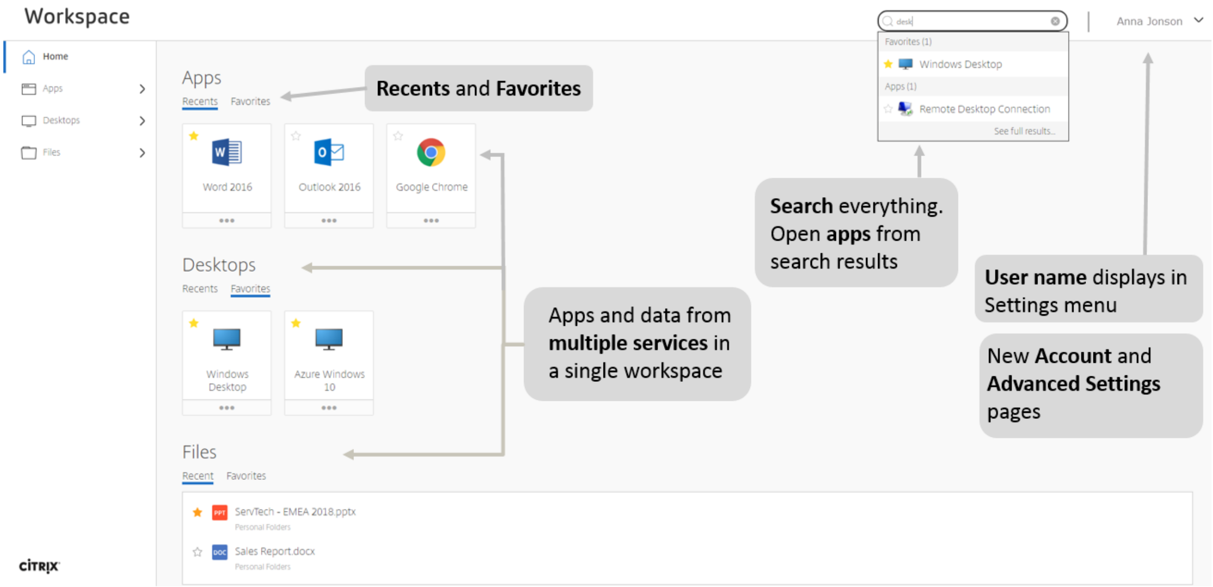
To close Citrix Workspace, use **Settings > Log Off**. That option completes the sign-out process from the workspace and Azure AD. If subscribers close the browser instead of using the **Log Off** option, they might remain signed in to Azure AD.

Copied!
Failed!

Manage your workspace experience

March 12, 2020

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



Recents and Favorites

Search everything. Open **apps** from search results

Apps and data from **multiple services** in a single workspace

User name displays in Settings menu

New **Account** and **Advanced Settings** pages

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 currently 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.

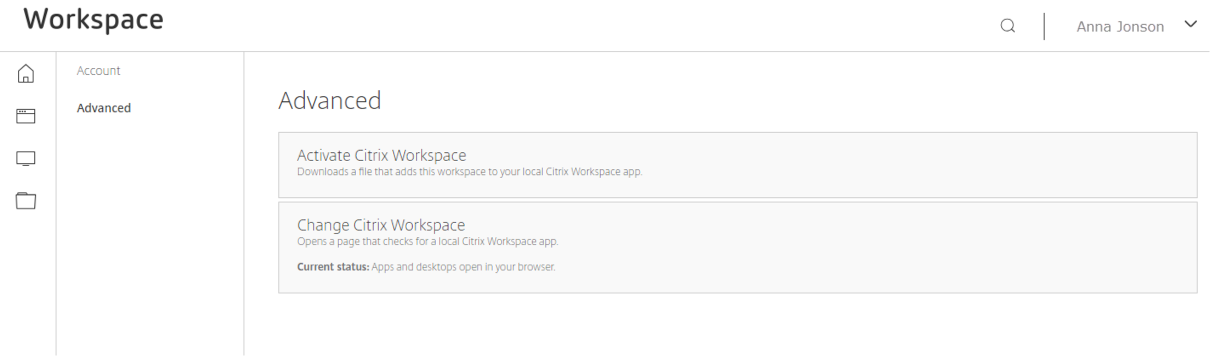
Favorites

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.



Advanced

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.

Current status: Apps and desktops open in your browser.

- **Activate Citrix Workspace**. Downloads a file that adds this workspace to your local Citrix Receiver app.

- **Change Citrix Workspace**. Opens a page that checks for a local Citrix Workspace app. Not available in Internet Explorer 11.

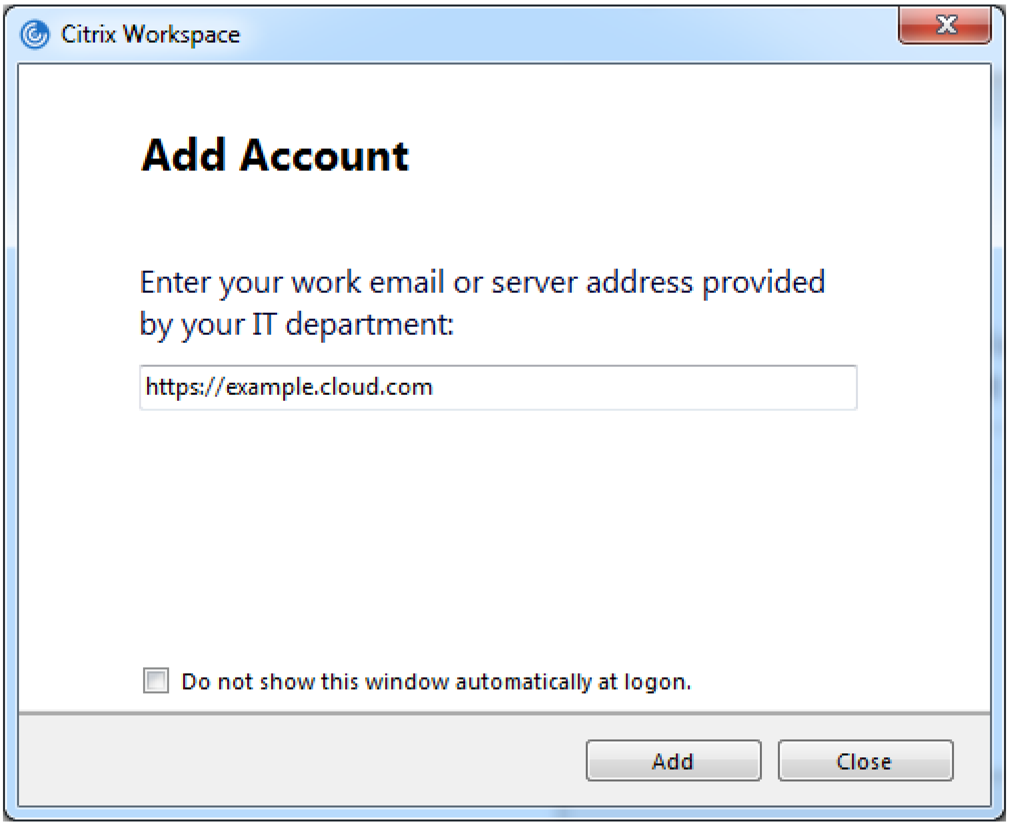
  > **Note:**
  >
  > This option is only available with Citrix Virtual Apps and Desktops services. **Change Citrix Workspace** is not available if, for example, you are only using SaaS apps through the Citrix Gateway service.

- **Download Citrix Workspace**. Downloads a Citrix Receiver 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 click **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`.


Citrix Workspace
Add Account
Enter your work email or server address provided by your IT department:
https://example.cloud.com
□ Do not show this window automatically at logon.
Add
Close

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.

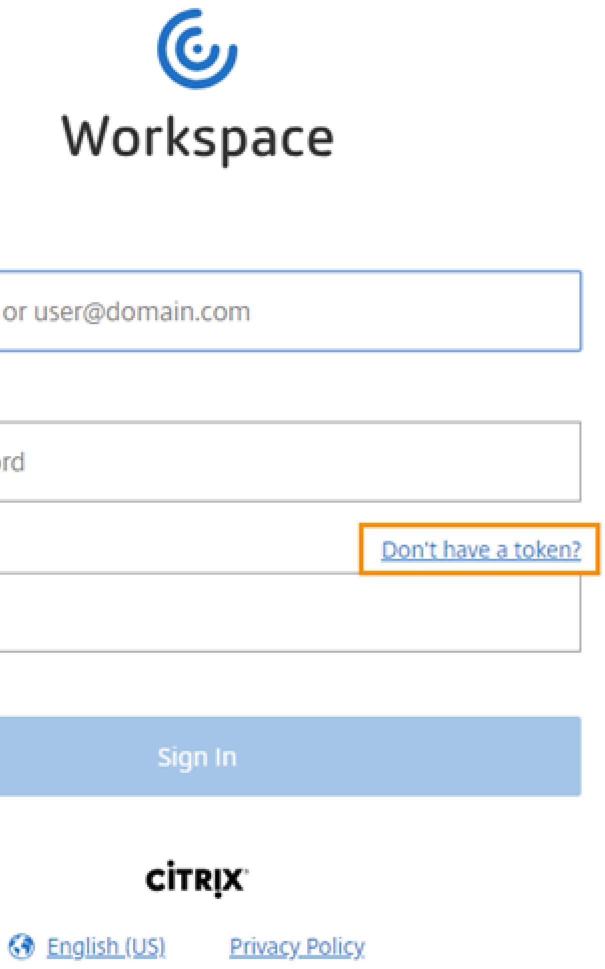
Errors from authentication changes

If an administrator makes a change to the authentication method - for example, from Active Directory to Azure Active Directory - subscribers who are logged on to Citrix Workspace may see errors in Citrix Workspace. If this happens, log off Citrix Workspace and close the browser or Citrix Workspace app. Wait approximately 5 minutes and log back on again. Citrix Workspace should be available again. You can log on using the new authentication method.

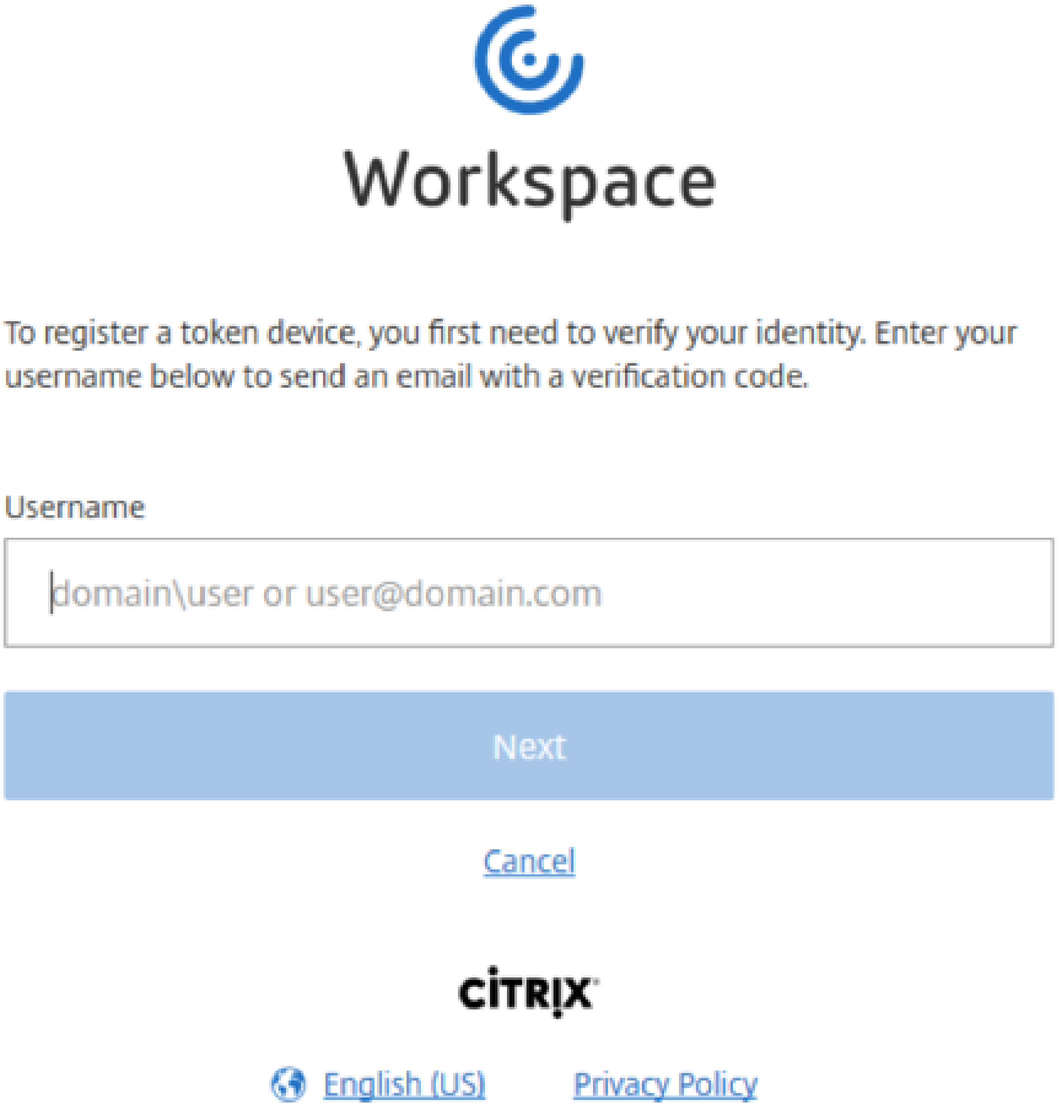
Register devices for two-factor authentication

Before subscribers can use two-factor authentication plus token with Workspace, they must first register their device. During registration, Workspace presents a QR code that subscribers can 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 click **Don't have a token?**



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



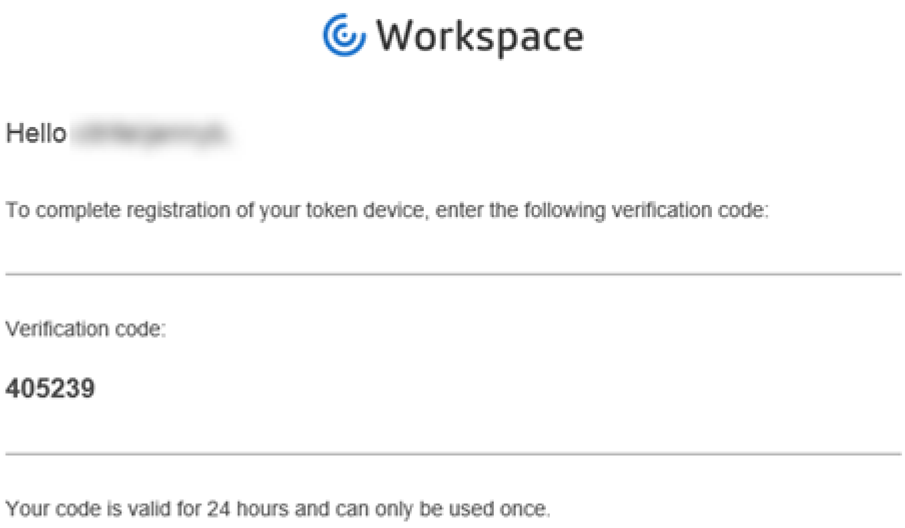
Workspace

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

domain\user or user@domain.com

Citrix Cloud sends you an email with a verification code.



Hello [redacted]

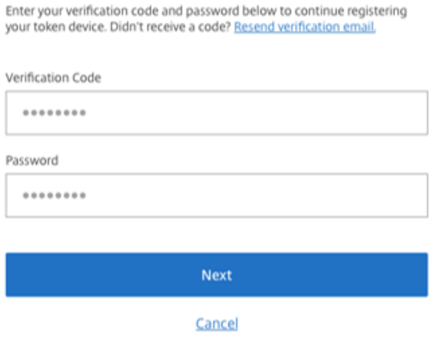
To complete registration of your token device, enter the following verification code:

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. Click **Next**.

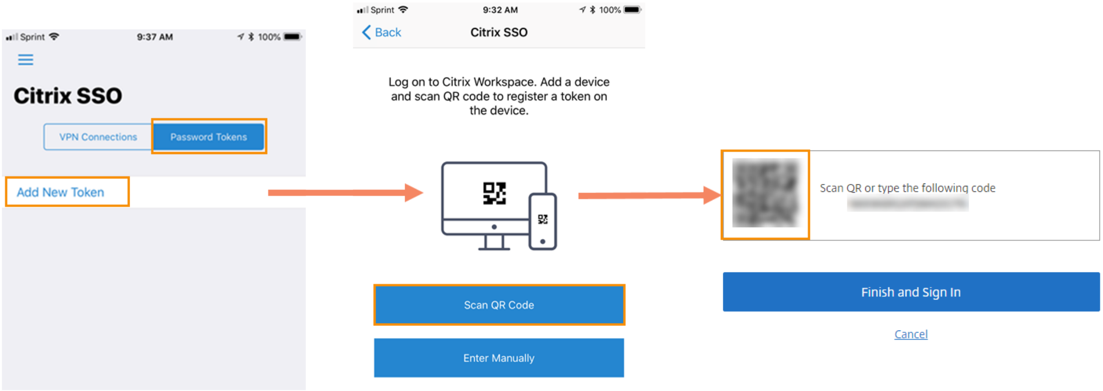


Enter your verification code and password below to continue registering your token device. Didn't receive a code? Resend verification email

Verification Code: ••••••••

Password: ••••••••

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

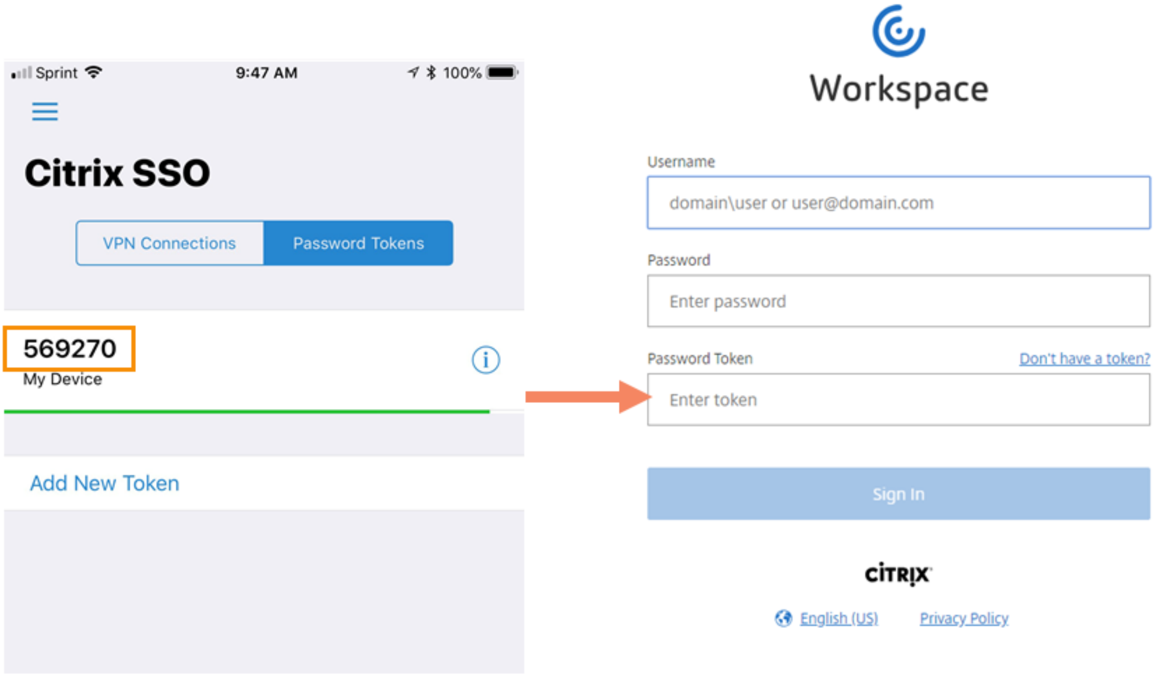


Log on to Citrix Workspace. Add a device and scan QR code to register a token on the device.

Scan QR or type the following code [redacted]

5. Click **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.



Copied!
Failed!

Citrix Assistant

April 2, 2020

Contributors

Special Thanks: Nikos Takoulis and Tomas Werner

What is Citrix Assistant?

Citrix Assistant is a virtual assistant available with Citrix Workspace. It provides an easy medium to accomplish tasks such as viewing employee information, finding expense reports, and finding tickets.

The virtual assistant pulls data from connected applications and helps you quickly find the information you need. It uses automated intelligence, machine learning capabilities, and natural language processing to understand the app context, conversation context, and user intent.

Why Citrix Assistant?

The time employees spend looking for internal information, learning how to use new applications, and context switching between apps can lead to a loss of productivity. Low productivity has a negative impact on employee engagement.

The Citrix Workspace virtual assistance feature improves employee engagement and productivity by providing immediate access to relevant content and business data.

Three key benefits of the virtual assistance feature are:

- Keeps the user experience simple by using a natural, conversational style.
- Improves employee engagement by reducing the number of context switches, logons, searches, and click-throughs.
- Enhances productivity by finding information quickly within the user's context, and by automating repetitive routine tasks.

How to access Citrix Assistant?

You can interact with Citrix Assistant from any endpoint that is enabled by Citrix Workspace:

- from the Citrix Workspace app on any device.
- from within an application context such as Microsoft Teams.

From Citrix Workspace, click the **Citrix Assistant** icon to start using its capabilities.

Citrix Assistant supports various skills such as a directory skill (Who does that person report to again?), a PTO skill (How many PTO days does an employee have left this year?), a learning courses skill (What courses are available to an employee?), and many more.

For a complete list of available skills, click the **Skills** menu on the **Citrix Assistant** interface.

Supported apps

Citrix Assistant supports the following apps:

- Concur
- JIRA
- MS Dynamics
- Salesforce
- SAP Ariba
- SAP SuccessFactors
- ServiceNow
- Workday
- Zendesk

Terminology

Citrix Assistant is offered as a feature of Citrix Workspace. To familiarize yourself with Citrix Workspace, see Citrix Workspace documentation.

- **Skill**: A rich set of capabilities provided by the virtual assistant to the users of the Workspace clients. The skills enable end user conversations with the virtual assistant. This allows the user to perform a specific query or task on the available SaaS applications/System of Records. For example, skills include PTO, Email, Calendar, and Company Directory.
- **Utterance**: A phrase entered into the Citrix Assistant by the end user querying for information from the assistant. For example, "show my team's time-off requests" is an utterance. The user expects the assistant to provide with the appropriate information in response to an utterance.
- **Response**: The answer provided to the end user in response to the utterance. It is based on the intent that the virtual assistant processes. A response might include data from the appropriate System of Records or other responses to help the user supply the proper phrasing to achieve their true intent.
- **Intent**: A pre-defined set of questions that users might ask the Citrix Assistant. Each intent is a use case or workflow that a natural language request translates into. For example, "who is Billy Taylor" would translate into the intent Directory.Lookup.
- **Entity**: An intent modifier used by the virtual assistant to provide the user with personalized and accurate responses. Entities help the virtual assistant to extract important information from the natural language input such as phone numbers, names, and places. For example, in the utterance "show all time-off requests pending my approval" the entities are "all," "pending," and "my."
- **Microapps**: Small, task-specific applications that deliver highly targeted functionality. These apps allow users to accomplish single-purpose activities in a simple and quick manner. Microapps deliver actionable forms and notifications. Microapps can write back to source systems.
- **Microapps service**: Refers to several components inside Citrix Cloud focused on delivering actions from your applications into your Workspace or other channels. Microapps service includes the microapps administrator, the microapps server, and cache.
- **Resolver**: Provides the configuration of the mapping between the virtual assistant's natural language understanding and the API calls to microapps API. Citrix assistant resolvers on the Microapps service are required to process the queries sent from the assistant to the microapp. The resolver retains specific data sent from the microapps database to the assistant. When you create an integration in the Microapp service, the Citrix assistant resolvers are configured by default. You can edit these resolvers and you can also add new resolvers.

How Citrix Assistant works

Citrix Assistant uses machine learning and automated intelligence to parse natural language into structured language and retrieve the requested information.

The following image shows the high-level steps that the virtual assistant takes to get information to end users.

As shown in the preceding image,

1. The user sends a request to the virtual assistant in natural language. For example, "show my time-off requests."
2. The virtual assistant then sends the request to a service to parse it into intent and entities.
3. Next, the virtual assistant sends the parsed text to another service to resolve the context, for example, what does "my" mean.
4. The virtual assistant communicates with the Microapps service to retrieve intent-specific information.
5. The Microapps service queries the cache database to retrieve the requested information. For information about the Microapps service, see Microapps.
6. Citrix Assistant resolvers, pre-configured on the Microapps service for each integration, process the queries sent from the virtual assistant to the Microapps service.

> **Note**
>
> For information about Citrix Assistant resolvers and how to edit or add resolvers, see Configure Citrix Assistant resolvers.

Architecture and process flow

The virtual assistant architecture includes different µ-services. Citrix maintains all components and hosts them within the Citrix Cloud control plane. The following components and µ-services are used by the virtual assistant.

- **Endpoints**: Enables users to interact with Citrix Assistant. You can interact with Citrix Assistant from any endpoint that is enabled by Citrix Workspace:
  - from the Citrix Workspace app on any device.
  - from within an application context such as Microsoft Teams.
- **Bot µ-service**: Manages all end user requests and sessions. It routes all utterances or events to appropriate µ-services to fulfill the requests and return a response to the end user.
- **Utterance µ-service**: Uses natural language processing (NLP) to understand and extract the meaning of a user utterance (request). An example of a user utterance is "show my time-off

requests.” The user interacts with the virtual assistant using natural language. However, at the back end, this language must be understood, processed, and structured to retrieve the correct response for the end user. The utterance µ-service performs the following activities:

  - Processes text utterances to perform spellcheck.
  - Communicates with the NLU µ-service to extract the intent and entities of the utterance.
  - Processes the intent and entities and presents them in an acceptable format by the other µ-service.

- **Spellcheck µ-service**: Corrects anything that is misspelled in the user’s natural language request.
- **Language models**: Detects intents of and parses entities from the user utterances.
- **Skills µ-service**: Manages dialogs and conversations with the user by fetching specific data from the Microapps service to create a response.
- **Microapps service**: Refers to several components inside Citrix Cloud focused on delivering actions from your applications into your Workspace or other channels. This is responsible for providing information to the virtual assistant.

The following image shows the high-level architecture and process flow for the virtual assistant:

Pre-requisite to using Citrix Assistant

Before end users can use Citrix Assistant from any of the endpoints, you must do the following:

- Enable Microapps service on Workspace. For more information, see Getting started with Microapps.
- Ensure that pre-configured Citrix Assistant resolvers are available with the app integrations.

Configuring Citrix Assistant resolvers

The Citrix Assistant resolvers process the queries sent from the virtual assistant to the microapp. A resolver includes the configuration of the mapping between the assistant’s natural language understanding and the API calls to Microapps.

When you create an integration in the Microapps service, the Citrix Assistant resolvers are configured by default. You can modify these resolvers and you can also add new resolvers.

> **Note**
>
> For information about Citrix Assistant resolvers and how to edit or add resolvers, see Configure Citrix Assistant resolvers

Authentication and authorization

The end user authenticates to Citrix Workspace to interact and engage with the virtual assistant. Communication between services in the back end is encrypted using TLS encryption 1.2 or above. The bot µ-service, the skills µ-service, and the Microapps service uses RSA key pairs with one-time tokens to enable trust between the services. The authorization path must be implemented on the Microapps service platform.

For information about Microapps service security and service authentication, see:

- Technical security overview
- Set up service authentication

Working with Citrix Assistant

The availability of Citrix Assistant on any device helps you take care of many tasks on the go and between meetings. It eliminates the need to launch your application, remember your sign-on information, or navigate to the required information.

Consider a scenario where Amy is the manager in a company and her organization uses Workday to track time-off details.

Amy wants to view time-off requests submitted by her team and pending her approval. Instead of launching and signing in to Workday, she uses Citrix assistant and types in natural language "show all time-off requests pending my approval." Citrix assistant immediately shows her the list of all pending time-off requests.

Amy can also click **View** to see more details of each time-off request. In this example, she can view details such as date when the request was submitted and the reason for the time-off request.

If Amy wants to view time-off request of an employee, she can type "find billy taylor's time-off request" and get the information immediately. To see more information such as the reason for the time-off request, she can click **View Details**.

> **Note**
>
> Before your employees begin using the virtual assistant, you must ensure Citrix Assistant resolvers are configured on the Microapps service. For more information, see Configure Citrix Assistant resolvers

Copied!
Failed!

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