Citrix Workspace
Contents

Citrix Workspace Overview 3
What’s New 7
Get started with Citrix Workspace 12
Deliver Virtual Apps and Desktops with Citrix Workspace 15
Access and share files with Content Collaboration in Citrix Workspace 18
Prepare for Citrix Workspace 21
Configure access to workspaces 27
Secure workspaces 36
Integrate services into workspaces 44
Manage your workspace experience 46
Customize workspace notifications 53
Customize the appearance of workspaces 58
Customize workspace interactions 64
Customize security and privacy policies 74
Optimize Virtual Apps and Desktops in Citrix Workspace 85
Aggregate on-premises virtual apps and desktops in workspaces 86
Optimize connectivity to workspaces with Direct Workload Connection 96
Service continuity 107
Fall back to StoreFront 130
Enable single sign-on for workspaces with Citrix Federated Authentication Service 136
Optimize workflows 148
IT Self-service 152
HR Self-service 154

© 1999–2022 Citrix Systems, Inc. All rights reserved.
Citrix Workspace

Sales Productivity 156
Employee Well-being 158
Citrix Workspace Overview

January 21, 2022

Citrix Workspace is a digital workspace solution that delivers secure and unified access to apps, desktops, and content (resources) from anywhere, on any device. These resources can be Virtual Apps and Desktops, content apps, local and mobile apps, SaaS and Web apps, and browser apps.

How Citrix Workspace works

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

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

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

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

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

Get started overview

Citrix Workspace is set up through the Citrix Cloud console, in which there’s an Identity and Access Management administration screen and a Citrix Workspace management interface called Workspace Configuration. Getting started with Citrix Workspace involves the following tasks.

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

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

• Configure single sign-on (SSO) to virtual apps and desktops in Citrix Workspace with the Citrix Federated Authentication Service (FAS). FAS is typically adopted if you’re using a federated authentication method, such as Okta or Azure Active Directory.
• Optimize workflows with microapp templates to create actionable notifications in Citrix Workspace Actions and in the Activity Feed.

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

Cloud-hosted services through Citrix Workspace

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

with them into the Citrix Workspace solution.

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

**Citrix Virtual Apps and Desktops service**

Citrix Workspace is the multitenant, cloud-hosted access point to Citrix Virtual Apps and Desktops. To set up the Citrix Virtual Apps and Desktops service, follow the steps outlined in Citrix Virtual Apps and Desktops service.

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

**Citrix Content Collaboration for secure file access, sharing, and collaboration**

**Citrix Content Collaboration** delivers Citrix ShareFile alongside other offerings, such as Citrix RightSignature for paperless document signing, and the App Builder, powered by Citrix Podio.

Existing ShareFile customers can link their account to Citrix Cloud with Content Collaboration. This allows end users to access and collaborate on content through the Files tab in the Workspace UI or Citrix Files app.

To take advantage of Content Collaboration in Citrix Workspace, you must:

1. Have an entitlement to Content Collaboration or ShareFile.
2. Link your existing ShareFile entitlement or enable a new Content Collaboration entitlement.
3. Enable Content Collaboration in Citrix Workspace. See Deploy and enable Citrix Content Collaboration in Citrix Workspace.

Once this process is complete, subscribers see the Files tab in the left-side navigation of the Citrix Workspace UI.

The exact steps and the order in which you follow them depend on your starting point and desired end state.

- **Create a new Content Collaboration account.** Allow subscribers to access content through Citrix Workspace with a new Content Collaboration account.
- **Add an existing ShareFile account to a new Workspace deployment.** Set up Citrix Workspace as an existing ShareFile customer by adding an existing ShareFile account to a new Workspace deployment.

© 1999–2022 Citrix Systems, Inc. All rights reserved.
• Add an existing ShareFile account to an existing Workspace deployment. If you’re an existing ShareFile customer that already has Citrix Workspace configured, create a unified experience by adding an existing ShareFile account to an existing Workspace deployment.

For an overview of the steps involved, visit Access and share files with Content Collaboration through Citrix Workspace.

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

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

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

Citrix Gateway service

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

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

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

Citrix Secure Browser service

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

To give subscribers access to a secure browser, set up the Secure Browser Service, and then test and share the Workspace URL with your subscribers.

Citrix Endpoint Management

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

**Citrix Analytics**

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

**Microapps service**

Citrix Workspace generates relevant notifications, tasks, and insights that are intelligently targeted at each subscriber through the **Activity Feed** and the **Actions** card in their workspaces.

The **Microapps service** is the mechanism behind notifications and optimized actions. The service uses microapps (workflows) to communicate with, and write back to, source systems. Subscribers can then view notifications and perform actions without leaving their workspaces.

For more information on the subscriber experience of **Actions** and the **Activity Feed** in Workspace, visit Manage your workspace experience.

For information on enabling and rolling out targeted notifications, tasks, and insights, visit Configure and rollout workspace notifications.

For easy deployment, Citrix recommends adding integrations from a selection of integration templates. For more information on connecting out-of-the-box integration templates with Citrix Workspace, see Optimize workflows. For more advanced options that require flexibility, you can create an HTTP integration. You can also import a previously configured integration, allowing you to save development time and replication of work.

For more information about getting started with the **Microapps service**, visit Getting started.

**What’s New**

March 2, 2022

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

This process is transparent to you. Initial updates are applied to Citrix internal sites only and are then applied to customer environments gradually. Delivering updates incrementally maximizes product quality and availability.
For details about the Service Level Agreement for cloud scale and service availability, see the Citrix Cloud Service Level Agreement. To monitor service interruptions and scheduled maintenance, see the Service Health Dashboard.

February 2022

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

Custom banners and custom sign-in policy: Two new features are now available for all customers. These features allow Workspace administrators to display their own post-login persistent banner and pre-login custom message or license agreement in Citrix Workspace app. For more information, see Customize security and privacy policies.

December 2021

Remove the default, split sign-in screen for employee and client users of Citrix Content Collaboration: Citrix Workspace now allows you to enable a single sign-in flow for both client and employee users. For more information, see Create a unified user sign-in flow.

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

November 2021

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

October 2021

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

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

**September 2021**

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

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

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

**July 2021**

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

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

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

**June 2021**

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

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

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

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

**May 2021**

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

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

**February 2021**

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

**December 2020**

**Service continuity technical preview:** Service continuity allows users to connect to their virtual apps and desktops even during outages in Citrix Cloud components or in public and private clouds. For more information, see Service continuity.
October 2020

**FedRAMP Ready:** Citrix Workspace is FedRAMP Ready when deployed in Citrix Cloud Government. FedRAMP is a program that promotes security standards for cloud services used by US government organizations. US government organizations that require FedRAMP Ready cloud services can now use Citrix Workspace and Citrix Virtual Apps and Desktops services to deliver virtual apps and desktops. For more information, see [Citrix Cloud Government](#).

June 2020

**Controlled feature rollout for Actions and the Activity Feed:** With the Customize > Features tab in Workspace Configuration, you can ensure that 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 for workspace authentication, you can roll out **Actions** and the **Activity Feed** to select users and groups or to all subscribers with access to microapps. For more information, see [Actions and the 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 and quick access to the instructions you need, see [Get Started with Citrix Workspace](#).

December 2019

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

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

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

January 26, 2022

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

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

- Extending workspaces with the Files tab when you enable Citrix Content Collaboration.
  - If you want to create a new Content Collaboration account for your Workspace deployment, visit Create a new Content Collaboration account.
  - If you want to link an existing ShareFile account to a Workspace deployment, visit Link your Citrix ShareFile account.
- Delivering Citrix Virtual Apps and Desktops through workspaces.
  - If you want to access resources in your on-premises Virtual Apps and Desktops deployment through Workspace, see Site aggregation for hybrid solutions.
  - If you want to migrate to the cloud, see Full migration to the cloud.

Workflow overview

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

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

The Success Center provides additional solution-based guidance.

Phase 1: Prepare for Citrix Workspace in Citrix Cloud

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

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

The steps involved in Phase 1 include:

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

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

**Phase 2: Configure subscriber access and authentication**

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

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

**Note:**

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

For more information, visit **Workspace access**.

**Configure workspace access**

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

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

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

**Configure subscriber authentication to workspaces**

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

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

If you’re using a federated identity provider, you can also enable single sign-on (SSO) to virtual apps and desktops with the **Citrix Federated Authentication Service (FAS)**.

For more information on configuring subscriber authentication to workspaces, visit [Secure workspaces](#).

**Phase 3: Integrate services into workspaces**

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

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

**Phase 4: Customize workspaces**

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

- Configuring targeted notifications and tasks in the **Activity Feed** and **Actions** card of workspaces. For information on enabling and rolling out personalized notifications in workspaces, visit [Customize workspace notifications](#).
- Customizing the appearance of workspaces, including logos and custom themes. For instructions on customizing Workspace appearance, visit [Customize the appearance of workspaces](#).
- Choosing interaction options, such as allowing subscribers to create **Favorites** and automatically launching desktops. For instructions on customizing how subscribers interact with their workspaces, visit [Customize workspace interactions](#).
- Customizing privacy and security, including setting a timeout period, creating a sign-in policy, and allowing subscribers to change their passwords from within their workspaces. For instructions on how to customize Workspace privacy and security policies, visit [Customize security and privacy policies](#).

**Phase 5: Roll out Citrix Workspace to subscribers**

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

1. Testing workspaces.
• Verify that you can sign in through the browser and into the Citrix Workspace app.
• Launch and use all available apps and desktops.
• Check that you can access available folders and files.
• Check that notifications are displaying the expected actions and activities.
• If enabled, verify that you can access endpoint resources on mobile devices.

2. Onboarding subscribers.
   • Communicate Citrix Workspace capabilities with subscribers.
   • Share the browser Workspace URL.
   • Guide users to install the Citrix Workspace app.

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

Deliver Virtual Apps and Desktops with Citrix Workspace

January 19, 2022

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

You have different options for aggregating your Virtual Apps and Desktops with Citrix Workspace. The option you choose depends on:

• Whether you want to fully migrate to the cloud or to adopt a hybrid solution.
• Whether you plan to allow external access to Virtual Apps and Desktops.

Full migration to the cloud

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

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

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

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

Site aggregation for hybrid solutions

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

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

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

There are three broad steps involved in site aggregation:

1. Discover site. A site comprises the components that make up a production deployment. You might have different sites for different locations and branch offices.

2. Verify Active Directory (AD) connection. Subscribers must authenticate to Citrix Workspace with AD. Ensure that subscribers can authenticate by detecting the AD domains in which your Cloud Connectors are installed.

3. Choose deployment type. There are three connectivity options for this step:
   - IT-managed gateways
   - Citrix-managed gateways
   - No gateway

For more information, see Connectivity options.

Connectivity options

The following three options provide access to Virtual Apps and Desktops through Citrix Workspace, designed for different business requirements.
## Connectivity option

<table>
<thead>
<tr>
<th><strong>Traditional (IT-managed) gateways</strong></th>
<th>Choose this option if you’d like to use your own gateway for external connectivity to your Virtual Apps and Desktops. This allows you to take advantage of your current investment in on-premises gateways.</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Citrix-managed gateways</strong></td>
<td>Choose this option if you’d like to use the <a href="#">Citrix Gateway service</a> for external connectivity to your virtual apps and desktops. HDX connections between clients and VDAs are proxied through the <a href="#">Citrix Gateway service</a>.</td>
</tr>
</tbody>
</table>
## Connectivity Option Scenario

<table>
<thead>
<tr>
<th>Connectivity option</th>
<th>Scenario</th>
</tr>
</thead>
<tbody>
<tr>
<td>No gateway (internal only)</td>
<td>Choose this option if you want subscribers to launch to Virtual Apps and Desktops only using clients inside your corporate network. Subscribers won’t have external access to Virtual Apps and Desktops if you choose this option.</td>
</tr>
</tbody>
</table>

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

### Configure Workspace Resiliency and Optimization

For information on improving the efficiency and availability of your virtual apps and desktops through Citrix Workspace, visit [Optimize Virtual Apps and Desktops in Citrix Workspace](#). Citrix provides instructions on how to:

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

**Note:**

You can’t use service continuity and fall back to StoreFront together. Choose the resiliency option that is best suited to your organization’s needs.

### Access and Share Files with Content Collaboration in Citrix Workspace

January 5, 2022

Citrix Content Collaboration provides business-class file sharing, streamlined workflows, and real-time collaboration in one location. The service unifies content from cloud and on-premises storage through the Citrix Workspace UI, with support for customer-managed and third-party cloud repositories.

Existing Citrix ShareFile customers can link their account to Citrix Cloud through Content Collaboration. The end user can then access and collaborate on content using the **Files** tab in the Workspace UI or through the **Citrix Files app**.
To access and share files with Content Collaboration, you must first have a Citrix Cloud account and purchase the relevant licenses.

Getting started with Content Collaboration in Citrix Workspace

To make the Files tab available in Citrix Workspace, you must integrate and enable a Citrix Content Collaboration account in Workspace Configuration. The steps involved depend on your starting point and desired end state.

- **Existing ShareFile customers.** If you’re an existing ShareFile customer, you can provide access to the same content through the Files tab in Citrix Workspace. For an overview of what this involves, see Link your Citrix ShareFile account.

- **New Content Collaboration customers.** If you’re not an existing ShareFile customer, you must instead create a new Content Collaboration account that you can then access through the Files tab in Citrix Workspace. For an overview of what this involves, see Create a new Content Collaboration account.

For more information on linking to Citrix Cloud, visit Create or link a Content Collaboration (ShareFile) account to Citrix Cloud.

Create a new Content Collaboration account

Choose this route if you want to create a new Content Collaboration account for a unified experience of apps, desktops, and content. Broadly, the steps involved include the following:

1. Configure authentication for Citrix Workspace, which is the two-step process described in Configure subscriber access and authentication.
2. Create a new Content Collaboration account and assign your Content Collaboration entitlements to that account, as described in Create a new Content Collaboration account and assign entitlements.

If you don’t have an identity provider, you must create a ShareFile account instead, and then follow the steps outlined in Add an existing ShareFile account to a new Workspace deployment under Link your Citrix ShareFile account.

Link your Citrix ShareFile account

To allow users access to ShareFile content through Citrix Workspace, you must first link your ShareFile account with Citrix Cloud. You can preview this experience by manually moving to “testing mode” for initial integration. Subscribers can now choose whether they access their content through the Files tab in Citrix Workspace or with their existing ShareFile account.
Full migration to the cloud involves manually moving from testing mode to full integration. Subscribers then access content only through Citrix Workspace, alongside other services that you enable for their workspaces.

Alternatively, if you have any existing ShareFile accounts that you want to assign to a new Content Collaboration account, follow the steps outlined in Create a new Content Collaboration account.

**Add an existing ShareFile account to a new Workspace deployment**

Choose this route if you’re setting up Citrix Workspace for the first time as an existing ShareFile customer.

1. Configure identity providers for subscriber authentication to Citrix Workspace. For information on configuring authentication to Citrix Workspace, visit Secure workspaces.
2. Link your ShareFile account to Citrix Cloud. Select Link Account under the Add Service drop-down menu in the Content Collaboration tile in Citrix Cloud, then choose the account you want to link to Citrix Workspace.
3. Enable the Workspace URL in Workspace Configuration > Access. For information on enabling and editing the Workspace URL, see Workspace URL.
4. Move into testing (preview) mode for initial integration. Enable Content Collaboration in Workspace Configuration > Service Integrations.

**Add an existing ShareFile account to an existing Workspace deployment**

Choose this route if you’d like subscribers to access ShareFile content through an existing Workspace deployment, for which access and authentication is already be configured. If you haven’t configured an identity provider and authentication method for accessing workspaces, follow the steps outlined in Add an existing ShareFile account to a new Workspace deployment.

1. Select Link Account under the Add Service drop-down menu in the Content Collaboration tile in Citrix Cloud, then choose the account you want to link to Citrix Workspace.
2. Move into testing (preview) mode for initial integration. Enable Content Collaboration in Workspace Configuration > Service Integrations.
Prepare for Citrix Workspace

January 14, 2022

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

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

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

The Citrix Cloud product documentation offers more detailed guidance for IT managers and developers into the pre-requisites and activities involved in preparing for Citrix Workspace in Citrix Cloud.

System and connectivity requirements

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

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

In sum, Citrix Cloud requires the following configuration:

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

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

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

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

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

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

**Plan your deployment and rollout**

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

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

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

**Sign in or sign up to Citrix Cloud**

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

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

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

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

**Add administrators**

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

**Invite administrators**

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

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

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

**Set up administrator authentication**

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

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

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

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

Instructions for setting up MFA can also be found in the Knowledge Center, and in Enroll in multifactor authentication in the Citrix Cloud product documentation.

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

**Edit administrator permissions**

To configure custom access to *Workspace Configuration*:

1. From the *Citrix Cloud* menu, select *Identity and Access Management* and then select *Administrators*.

2. Locate the administrator you want to manage, select the ellipsis button, and then select *Edit Access*.

3. Check that *Custom Access* is enabled.

4. To enable only *Workspace Configuration* access, select *Workspace Configuration* under *General Management*.
After enabling access, administrators can sign in to Citrix Cloud and select **Workspace Configuration** from the **Citrix Cloud** menu.
Check your entitlements

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

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

If you’d like to buy a new service, you can convert a trial into a production service without reconfiguration or creating a new account. To buy a service, take note of your organization ID in the top right corner of the Citrix Cloud console and visit https://www.citrix.com/product/citrix-cloud.
Set up the infrastructure

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

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

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

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

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

For more information, visit Citrix Cloud Connector.

Note:

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

Next: Build your workspace

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

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

Configure access to workspaces

January 27, 2022
Citrix recommends using the latest version of Citrix Workspace app to access workspaces. Citrix Workspace app replaces Citrix Receiver. You can also access workspaces using the latest version of Edge, Chrome, Firefox, or Safari with the Workspace URL.

Important:
Browser support for Internet Explorer ends on March 31, 2022.
Citrix recommends transitioning subscribers to the latest versions of Edge, Chrome, Firefox, or Safari before this date.

This article summarizes the steps involved in configuring and using:

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

Overview

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

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

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

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

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

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

Citrix Workspace also supports the following authentication options:

- Tokens as a second factor of authentication for signing in to workspaces with Active Directory. For more information on setting up multifactor authentication to workspaces, see Two-factor authentication.
Citrix Workspace

- Citrix Federated Authentication Service (FAS) to provide single sign-on (SSO) to virtual apps and desktops in Citrix Workspace. For more information on setting up SSO with FAS, see Enable single sign-on for Workspaces with Citrix Federated Authentication Service.

**Workspace URL**

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

![Workspace Configuration](image)

**Customize the Workspace URL**

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

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

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

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

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

- Must be between 6 and 63 characters long. If you want to change the customizable part of the URL to fewer than 6 characters, open a ticket in Citrix Cloud.
- Must consist of only letters and numbers.
- Can’t include Unicode characters.
When you rename a URL, the old URL is immediately removed and is no longer available.

If you change the Workspace URL, your subscribers can’t access their workspaces until the new URL is active, which takes about 10 minutes. Tell subscribers what the new URL is and manually update all local Citrix Workspace apps to use the new URL.

**Disable the Workspace URL**

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

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

Disabling the workspace URL has the following effects:

- All service integrations are disabled. Subscribers can’t access data and applications from services in Citrix Workspace.
- You can’t customize the Workspace URL. You must re-enable the URL before you can change it.
- Anyone visiting the URL receives a 404 message in their browser.

**Citrix Workspace app (formerly Citrix Receiver)**

Important:

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

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

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

<table>
<thead>
<tr>
<th>Citrix Workspace app</th>
<th>Active Directory Authentication</th>
<th>Active Directory plus Token Authentication</th>
<th>Azure Active Directory authentication</th>
</tr>
</thead>
<tbody>
<tr>
<td>Citrix Workspace for Windows</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes (Workspace app; Receiver 4.9 LTSR CU2 and later only; Receiver 4.11 CR and later only)</td>
</tr>
<tr>
<td>Citrix Workspace for Linux</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes (Workspace app; Receiver 13.8 and later only)</td>
</tr>
<tr>
<td>Citrix Workspace for Mac</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>Citrix Workspace for iOS</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>Citrix Workspace for Android</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes (Workspace app; Receiver 3.13 and later only)</td>
</tr>
</tbody>
</table>

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

For an overview of TLS and SHA2 support with Citrix Receivers, see theCTX23226 Support article.

Transition from Citrix Receiver to Citrix Workspace app

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

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

This access control feature isn’t supported in Citrix Receiver. Thus, with the same services and access control enabled, Citrix Receiver users still see the purple UI, but without Web and SaaS apps. Additionally, Files isn’t supported in Citrix Receiver and subscribers can’t access them this way.
Azure Active Directory (AAD) also isn’t compatible with Citrix Receiver. If subscribers attempt to access Workspace with Citrix Receiver when AAD is enabled as the authentication method, they see a message that the device isn’t supported. Once they upgrade to Citrix Workspace app, they can access their workspaces.

Customers that upgrade to Citrix Workspace app (or use a Web browser) see the new UI. For more
information on what the subscriber experience of this UI is, visit Manage your workspace experience.

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

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

Note:

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

External connectivity

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

Citrix supports the following external connectivity options:

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

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

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

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

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

Supported identity providers for authenticating subscribers

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

- Active Directory
- Active Directory plus token
- Azure Active Directory
Citrix Workspace

- Citrix Gateway
- Okta
- SAML 2.0

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

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

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

Changing identity providers

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

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

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

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

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

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

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

© 1999–2022 Citrix Systems, Inc. All rights reserved.
Single sign-on (SSO) to virtual apps and desktops

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

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

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

- Azure AD
- Okta
- SAML 2.0
- Citrix Gateway

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

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

Secure workspaces

January 26, 2022

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

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

These authentication options are available to any Citrix Cloud service.

Citrix Workspace also supports using Citrix Federated Authentication Service (FAS) to provide single sign-on (SSO) to virtual apps and desktops. SSO with FAS removes the need for subscribers to au-
Citrix Workspace

Authenticate to Virtual Apps and Desktops after already signing in to their workspaces using a federated authentication method. For more information, see Enable single sign-on for workspaces with Citrix Federated Authentication Service.

**Choose or change authentication methods**

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

**Important:**

Switching authentication modes can take up to five minutes and causes an outage to your subscribers during that time. Citrix recommends limiting changes to periods of low usage. If you do have subscribers logged on to Citrix Workspace using a browser or Citrix Workspace app, advise them to close the browser or exit the app. After waiting approximately five minutes, they can sign in again using the new authentication method.

**Active Directory (AD)**

By default, Citrix Cloud uses Active Directory (AD) to manage subscriber authentication to workspaces.

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

**Active Directory (AD) plus token**

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

Requirements for AD plus token

Active Directory plus token authentication has the following requirements:

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

First-time enrollment

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

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

Important:

During the device enrollment process, subscribers receive an email with a temporary verification code. This temporary code is used only to enroll the subscriber’s device. Using this temporary code as a token for signing in to Citrix Workspace with two-factor authentication isn’t supported. Only verification codes that are generated from an authentication app on an enrolled device are supported tokens for two-factor authentication.

Re-enroll a device

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

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

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

Azure Active Directory

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

- Azure AD with a user who has global administrator permissions. For more information on the Azure AD applications and permissions that Citrix Cloud uses, see Azure Active Directory Permissions for Citrix Cloud.
- A Citrix Cloud Connector installed in the on-premises AD domain. The machine must also be joined to the domain that is syncing to Azure AD.
- VDA version 7.15.2000 LTSR CU VDA or 7.18 current release VDA or higher.
- A connection between Azure AD and Citrix Cloud. For information, see Connect Azure Active
Directory to Citrix Cloud.

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

**Warning:**

- If you’re using Azure AD, don’t make the registry change described in [CTX225819](https://www.citrix.com/). Making this change might cause session launch failures for Azure AD users.
- Adding a group as a member of another group (nesting) isn’t 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. Don’t specify users and user groups when creating or editing Delivery Groups.
- **Added security:** For security, users are prompted to sign in again when launching an app or a desktop. The password information flows directly from user’s device to the VDA that is hosting the session.
- **Sign-in experience:** Azure AD authentication provides federated sign-in, not single sign-on (SSO). Subscribers sign in from an Azure sign-in page, and might have to authenticate again when opening Virtual Apps and Desktops.

For SSO, enable the Citrix Federated Authentication Service in Citrix Cloud. See [Enable single sign-on for workspaces with Citrix Federated Authentication Service](https://www.citrix.com/) 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 Workspace supports using an on-premises Citrix Gateway as an identity provider to manage subscriber authentication to workspaces.

Requirements for Citrix Gateway

Citrix Gateway authentication has the following requirements:

- A connection between your Active Directory and Citrix Cloud. For requirements and instructions, see Connect Active Directory to Citrix Cloud.
- Subscribers must be Active Directory users to sign in to their workspaces.
- If you’re performing federation, your AD users must be synchronized to the federation provider. Citrix Cloud requires the AD attributes to allow users to sign in successfully.
- An on-premises Citrix Gateway:
  - Citrix Gateway 12.1 54.13 Advanced edition or later
  - Citrix Gateway 13.0 41.20 Advanced edition or later
Citrix Workspace

- **Citrix Gateway** authentication enabled in the *Identity and Access Management* page. This generates the client ID, secret, and redirect URL required to create the connection between Citrix Cloud and your on-premises Gateway.
- On the Gateway, an OAuth IdP authentication policy is configured using the generated client ID, secret, and redirect URL.

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

**Subscriber experience of Citrix Gateway**

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

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

**Okta**

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

**Requirements for Okta**

Okta authentication has the following requirements:

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

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

**Subscriber experience with Okta**

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

1. The subscriber navigates to the Workspace URL in their browser or launches the Workspace app.
2. The subscriber is redirected to the Okta sign-in page and is authenticated using the method configured in Okta (for example, multifactor authentication, conditional access policies, and so on).

3. After successful authentication, the subscriber’s workspace appears.

Okta authentication provides federated sign-in, not single sign-on (SSO). Subscribers sign in to workspace from an Okta sign-in page, and might have to authenticate again when opening Virtual Apps and Desktops. For SSO, enable the Citrix Federated Authentication Service in Citrix Cloud. See Enable single sign-on for workspaces with Citrix Federated Authentication Service for more information.

**SAML 2.0**

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

**Requirements for SAML 2.0**

SAML authentication has the following requirements:

- SAML provider that supports SAML 2.0.
- On-premises Active Directory domain.
- Two Cloud Connectors deployed to a resource location and joined to your on-premises AD domain.
- AD integration with your SAML provider.

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

**Subscriber experience with SAML 2.0**

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

**Citrix Federated Authentication Service (FAS)**

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

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

**Subscriber sign-out experience**

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

---

**Important:**

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

---

**Integrate services into workspaces**

January 5, 2022

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

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

**Configure services**

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

To configure purchased services:

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

For a brief description of cloud-hosted services, visit **Cloud-hosted services through Citrix Workspace**.

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

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

Subscribing to the **Virtual Apps and Desktops service** and the **Secure Browser service** enables them by default. All other new services that your organization subscribes to are disabled by default.

---

**Note:**
Both the **Citrix Apps Essentials service** and the **Citrix Virtual Apps and Desktops service** display as “Citrix Virtual Apps and Desktops service” in the Service Integrations tab of Workspace Configuration.

To enable workspace integration for a service:

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

---

Disable services

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

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

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?

![Confirm button](image)

Manage your workspace experience

March 9, 2022

This article summarizes how subscribers access and interact with their workspaces and describes what subscribers see when they sign in to their workspaces. The article also summarizes options for customizing the workspace experience and offers guidance for common issues.

**Workspace access**

Subscribers can access Citrix Workspace in two ways:

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

**Browser access**

If using the browser, subscribers can access their workspaces with the Workspace URL and the latest versions of Edge, Chrome, Firefox, or Safari.
Important:
Browser support for Internet Explorer ends on March 31, 2022. Citrix recommends transitioning subscribers to the latest versions of Edge, Chrome, Firefox, or Safari before this date.

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

Citrix Workspace app access

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

The Citrix Workspace app is a natively installed app that replaces Citrix Receiver and provides a consistent user experience of the Workspace user interface (UI) across platforms. Citrix Workspace app is available for various operating systems. For details, see the Citrix Workspace app product documentation.

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

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

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

Workspace user interface and features

New customers. If you’re new to the workspace experience, subscribers get the latest version of the UI when it’s available.

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

**Single sign-on (SSO)**

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

**Card layout**

*Apps, Desktops, Files, Actions,* and the *Activity Feed* are presented in a “card” layout. A pop-up window shows more details and actions.

**Settings**

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

**Profile icon**

Subscribers can upload a picture to their profile. If no profile picture is set, the image defaults to an icon that is based on the subscriber’s Active Directory display name.
Search

The search tool at the top of the UI searches across all resources in the workspace and allows subscribers to open apps directly from the search results. Search requires at least three characters.

Recents and Favorites view

Subscribers can choose between a Recents and Favorites view of their apps, desktops, and files.
You can configure Favorites to make this feature available or unavailable to subscribers in Workspace Configuration. For more information on enabling and disabling the Favorites feature in Citrix Workspace, see Allow Favorites.

Actions and the Activity feed

Citrix Workspace delivers relevant notifications and tasks in the subscriber’s Activity Feed and in the Actions card of their workspaces. Subscribers can act on these targeted notifications without leaving their workspaces.
For more information on the subscriber experience of Actions and the Activity Feed, see Subscriber experience of notifications.

Subscriber experience of notifications

When you configure and enable the notifications feature, subscribers receive targeted, actionable, and searchable alerts and tasks in the Activity Feed and the Actions card of their workspaces.
For information on how to enable notifications in Citrix Workspace, see Customize workspace notifications.

Notifications in Citrix Workspace

When enabled, subscribers see personalized notifications in the Activity Feed in the center of their workspace. A subscriber can act on an item in this feed, such as approving a request, directly in the workspace. The Actions card on the right side of their workspace also provides quick access to common tasks like submitting expenses or creating a calendar event.
In the left navigation of the UI, the Actions tab displays all actions available to subscribers with access to microapps, such as links to other systems or intranet sites. The Feed tab in the left navigation of workspaces displays all alerts, such as company announcements or reminders.
Search notifications

Subscribers can search and filter microapp notifications and integrations, and act on notifications directly from their search results.

Note:

**Activity Feed** search is available in Workspace on Web and Desktop in US and EU accounts. **Activity Feed** search is offered as a public preview and isn’t currently HIPAA compliant.

Subscribers can use the search box at the top of the Workspace UI to enter a query.

Selecting **Feed** in the top menu gives all matching results. Subscribers can also filter results by **Status**, **Source**, **Action required**, and **Time period**.
Citrix Workspace

Search results for 'Citrix'

Feed

- **Citrix TIPs: Scoring an A+ with HTTP headers and Citrix Gateway**
  - Authored by: Michael McAlpine
  - 14 hours ago

- **Transition to a resilient, secure hybrid work model with Citrix and Google**
  - Authored by: Anudeep Athlur
  - 7 hours ago

- **New Course Available**
  - The eCWS-2024: Introduction to Citrix Secure Internet Access for Citrix Virtual Apps and Desktops Course has been released.
  - 23 days ago

- **New Course Available**
  - The eCNS-2024: Deploy Citrix SD-WAN through SD-WAN Orchestrator Course has been released.
  - 23 days ago

Filters

- Status
  - Dismissed: 0
  - Active: 4

- Source
  - Citrix Blogs: 2
  - Citrix Education: 2

Action Required

- Show only items that require action

Time Period

- Post year (4)

Subscribers can select any search result to open their notifications for more information and to complete any available actions.

Blog Post details

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

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

The post **Citrix TIPs: Scoring an A+ with HTTP headers and Citrix Gateway** first appeared on **Citrix Blogs**.

Related Stories

- Boost your performance with Citrix ADC
- Citrix TIPs: Moving off deprecated Citrix ADC features for Citrix Gateway
- The Citrix SD-WAN and Microsoft Azure Virtual WAN advantage

View Blog Post
Two-factor authentication (optional)

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

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

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

1. Open a browser, navigate to the Workspace sign-in page, and select Don’t have a token?
2. Enter their user name in the domain\username format or their company email address and select Next. Citrix Cloud then sends the subscriber an email with a temporary verification code.
3. Enter the verification code and Active Directory account password when prompted and select Next.
   IMPORTANT:
   The verification code is a temporary token with a 24-hour validity period and is only used to register the subscriber’s device. The subscriber mustn’t use this code to sign into their workspace with two-factor authentication.
4. From the authenticator app, scan the QR code or enter the verification code manually.
5. Select Finish and Sign In to complete the registration.

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

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

Customize workspaces

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

• To configure targeted notifications in the Activity Feed and Actions card of workspaces, visit Customize workspace notifications.
• To customize the appearance of workspaces, including logos and custom themes, visit Customize the appearance of workspaces.
• To choose how subscribers interact with their workspaces, such as allowing subscribers to create Favorites and automatically launching desktops, visit Customize workspace interactions.
• To customize privacy and security policies, including setting a timeout period, creating a sign-in policy, and allowing subscribers to change their passwords from within their workspaces, visit Customize security and privacy policies.

Troubleshooting

Log out and back in after changing authentication method

After you’ve changed the authentication method, subscribers that are logged in might see an error message. To rectify this, subscribers must log out of Citrix Workspace and close the browser or Citrix Workspace app, and wait approximately 5 minutes. When their workspaces are available again, the subscriber can sign in using the new authentication method.

For more information, visit Choose or change authentication methods.

Refresh after changes to your service subscription

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

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

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

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

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

Customize workspace notifications

January 25, 2022

Citrix Workspace delivers targeted notifications and actions that allow subscribers to do their work without leaving their workspaces.
The **Microapps service** generates notifications and actions from your app data sources (Systems of Record, SoR) and delivers them to Citrix Workspace through microapps. Microapps are workflows that you build to aggregate app tasks and resources.

Notifications are event-driven microapps that generate relevant alerts to display in the subscriber’s **Activity Feed**, such as task reminders and company news. Subscribers can view and act on these items directly in their workspaces.

You can also create user-initiated microapps to appear in the **Actions** card of workspaces. The microapps in the **Actions** card allow subscribers to complete tasks, like requesting time off or submitting a Help Desk inquiry, without leaving their workspaces.

To configure, enable, and roll out notifications, you must:

1. Configure the **Microapps service** in Citrix Cloud.
2. Enable Microapps in **Workspace Configuration > Service Integrations**.
3. Subscribe users and groups to your microapps in the **Microapp Integrations** page.
4. Enable and rollout the notifications feature in **Workspace Configuration > Customize > Features**.

**Step 1: Configure the Microapps service in Citrix Cloud**

Citrix Workspace comes with a preconfigured **Microapps service** subscription and is ready for you to start building microapps immediately. If you don’t yet have an entitlement to the **Microapps service** you can request a demo. For more information, visit [Onboard Microapps service](#).

You configure individual services, including the **Microapps service**, in **Citrix Cloud**. Sign in to **Citrix Cloud** and select **Manage** in the **Microapps** tile.
To configure the **Microapps service**, you must first integrate the apps you need for building your microapps (workflows). For information on configuring app integrations, visit **Set up template integrations**.

After integrating apps into Workspace, create the microapps that collect, process, and organize tasks and resources from your apps’ SoR to deliver targeted alerts and actions to subscribers. For more information on creating microapps, visit **Create microapps**.

**Step 2: Enable Microapps as a Service Integration in Workspace Configuration**

Enable the **Microapps service** in Workspace to allow subscribers to receive microapps. Enabling the **Microapps service** populates workspaces with the notifications and actions you configured in Step 1.

To enable the **Microapps service** in Citrix Workspace:

1. Navigate to **Workspace Configuration > Service Integrations**.
2. Select the ellipsis next to **Microapps**.
3. Select **Enable**.

For more information on enabling services in **Workspace Configuration**, visit **Enable services**.

**Step 3: Subscribe users and groups to microapps**

If you want to roll out notifications to select subscribers (Step 4), you must first create and subscribe users and user groups to the microapps that generate notifications in **Actions** and the **Activity Feed**.

For instructions, see **Manage subscribers** in the **Microapps** product documentation.

**Step 4: Customize roll out of notifications**

To enable alerts and tasks in the **Activity Feed** and **Actions** card of Citrix Workspace, you must decide how you want to roll them out in **Workspace Configuration > Customize > Features**. Here, you define whether you want to roll out notifications to all subscribers or to select user groups.

**Note**

To enable the notifications for specific users and groups, you must use one of the following authentication methods:

- Active Directory
Citrix Workspace

- Active Directory + Token
- Azure Active Directory
- Okta

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

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

1. Enable the feature in Workspace Configuration > Customize > Features.
2. Choose whether you want to enable the feature for selected users and groups or for everyone with a microapps subscription.
3. If you select Enable for selected users and groups, select the domain, and then search for the users and groups that see the notifications in their workspaces.
4. When you're finished adding users and groups, select Save.
To remove users or groups, under **Assign Users and Groups**, select the trash can icon for the user or group and then select **Remove**.
Customize the appearance of workspaces

January 12, 2022

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

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

<table>
<thead>
<tr>
<th>Logo</th>
<th>Required dimensions</th>
<th>Max. size</th>
<th>Supported formats</th>
</tr>
</thead>
<tbody>
<tr>
<td>Sign-in logo</td>
<td>350 x 120 pixels</td>
<td>2 MB</td>
<td>JPEG, JPG, or PNG</td>
</tr>
<tr>
<td>After sign-in logo</td>
<td>340 x 80 pixels</td>
<td>2 MB</td>
<td>JPEG, JPG, or PNG</td>
</tr>
</tbody>
</table>

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

Customize your default theme

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

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

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

**Note:**

Changes to the sign-in logo don’t impact users who authenticate to their workspace using third-party identity providers, such as Azure AD and Okta.

For information on how to customize an Azure AD sign-in page, see the Microsoft documentation. For information on how to customize the Okta-hosted sign-in page, see the Okta Developer documentation.

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

Customize the workspace appearance

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

Create multiple custom themes

Important:

This is a single-tenant feature. If your customer is a Citrix Service Provider tenant, it must have its own resource location, Cloud Connectors, and dedicated Active Directory domain. Citrix Service Provider tenants that share a resource location, Cloud Connectors, and dedicated Active Directory domain (multitenancy) aren’t currently supported.

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

Configure custom themes

To add your first custom theme under your default theme, select Add theme at the bottom left of the card under the Default appearance section.
If you already have at least one custom theme under the default theme, select **Add theme** at the top right of the list of existing themes.

1. Configure your custom theme:
   a) Upload your **Logo** (optional).
   b) Define your banner, accent, and text and icon **Colors** (optional).

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

3. Assign user groups to the theme:
   a) Select an identity provider, and its domain if prompted.
b) Search for the user group that you want to add to the custom theme.

c) Select the plus sign (+) button next to that group.

d) Repeat this process for each group that you want to add to your theme.

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

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

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

**Prioritize custom themes**

A user might belong to more than one user group, each of which might match to a different theme. You can define which theme a subscriber sees if they match to more than one by setting the priority of custom themes relative to one another.

**Important**

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

1. Select **Edit priority** at the top right of the list of themes, next to **Add theme**.
2. You can reorder the priority of themes in one of two ways:
   - Use the arrows on the right-hand side of each theme.
- Drag individual themes up and down the list using the handle on the left-hand side of the card.

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

**Customize workspace interactions**

January 12, 2022

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

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

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

**Allow Caching**

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

Caching is supported when accessing Citrix Workspace with a **supported web browser**. Caching isn’t available when using a locally installed Citrix Workspace app.

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

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

### Allow Favorites

Customers who have access to **Workspace Configuration** and the new Workspace experience can allow subscribers to favorite and unfavorite app and desktop resources. The **Allow Favorites** feature is enabled by default.

**Note:**

- For some existing customers (new to Workspace between December 2017 and April 2018), **Allow Favorites** defaults to **Disabled**. The administrator can decide when to enable this feature for their subscribers.
- **Allow Favorites** doesn’t affect the ability to favorite files. The ability to favorite files persists regardless of whether **Allow Favorites** is enabled or disabled in **Workspace Configuration**.

**The subscriber experience of Allow Favorites**

When enabled (default), subscribers can add up to 250 **Favorites** using the star icon at the top left-hand corner of each (non-mandatory) app and desktop card. The star changes from having no fill to a yellow fill when it’s favorited.
If a subscriber favorites more than 250 resources, the “oldest favorite” is removed (or as close as possible to preserve the most recent Favorites).

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

**App and desktop keywords**

Administrators can automatically add Favorite Apps for subscribers by using KEYWORDS: Auto and KEYWORDS: Mandatory settings in the Virtual Apps and Desktops service (Manage > Full Configuration > Applications).
• **KEYWORDS:Auto.** The app or desktop is added as a Favorite and subscribers can remove the Favorite.

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

**Note:**

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

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

• The subscriber sees only the Apps page in the left navigation pane in Workspace. The Favorite
Citrix Workspace

The Apps page doesn’t appear in the left pane because there’s no difference in the apps that appear on the Apps page and the Favorite page.

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

Automatically Launch Desktop

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

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

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

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

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

Opening Apps and Desktops

The Opening Apps and Desktops setting is available to customers who have access to Workspace Configuration and the new Workspace experience. The preference is available to new and existing customers. However, the introduction of this feature doesn’t change any settings for existing customers.

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

Choose one of the following settings:

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

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

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

Requirements

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

Enable Microsoft Teams integration

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

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

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

1. Sign in to any workspace account and try to share a card.

2. The following message appears if the Microsoft Administrator account hasn’t accepted permissions for integration with Microsoft Teams and you try to sign in with a non-administrator account:
3. To accept permissions, sign in to your administrator account by selecting **Have an admin account? Sign in with that account**. The following permissions to access data are required to enable the Microsoft Teams integration with Citrix Workspace:
4. When the Permissions accepted dialogue opens, review the options. The Consent on behalf of your organization grants permissions to all Workspace subscribers for this administrator. Otherwise, permissions are granted only for the administrator account.

5. Select Accept.
Citrix Workspace

Customize security and privacy policies

February 11, 2022

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

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

Create a unified user sign-in flow

If you have Citrix Content Collaboration configured, you can create both employee and client users for when employees frequently share content with users that are outside your organization. For more information on creating employee and client users for Citrix Content Collaboration, visit People settings.

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

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

---

**Set inactivity timeout for Web**

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

<table>
<thead>
<tr>
<th>Workspace Sessions</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Inactivity Timeout for Web</strong></td>
</tr>
<tr>
<td>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).</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>HOURS</th>
<th>MINUTES</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>20</td>
</tr>
</tbody>
</table>

Unlike manual sign-out, which disconnects virtual apps and desktops sessions, subscribers stay connected to their virtual apps and desktops sessions following timeout due to inactivity.
Set a reauthentication period for Citrix Workspace app

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

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

Reauthentication Period for Workspace App

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

Current Reauthentication Period: 1 Day(s) Edit

Learn more about Workspace reauthentication periods.

Save

By default, this setting requires subscribers to sign in every 24 hours (one day). You can specify a longer reauthentication period of up to 365 days. Longer reauthentication periods require subscriber consent to stay signed in.

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

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

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

Supported Workspace app clients

The following versions of Citrix Workspace app support this feature:

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

© 1999–2022 Citrix Systems, Inc. All rights reserved.
Supported authentication methods

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

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

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

Subscriber experience for staying signed in

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

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

If the subscriber selects **Deny**, Workspace prompts the subscriber to sign in again. Afterward, Workspace prompts the subscriber to sign in again after 24 hours have passed.
If the subscriber’s password changes, the subscriber must sign out and sign in again through Citrix Workspace app for the reauthentication period to continue to work.

**Allow subscribers to change their account password**

*Note:*

This feature is being rolled out to customers incrementally. You might not see the feature until the rollout process is complete.

Citrix aims to deliver new features and product updates to Citrix Workspace customers when they’re available. This process is transparent to you. Initial updates are applied to Citrix internal sites only, and are then applied to customer environments gradually. Delivering updates incrementally helps ensure product quality and maximize availability.

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

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

**Supported authentication methods**

- Active Directory
- Active Directory plus token

**Supported Workspace app clients**

The following versions of Citrix Workspace app support this feature:

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

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

This feature isn’t supported on older versions of Citrix Workspace app and Citrix Workspace app for Linux.
Password guidance

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

Important:

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

To add password requirements:

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

   Allow Account Password to be Changed
   
   ✅ Enabled

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

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

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

   ✖ Add a password requirement (20 max.)

   Save

4. Enter a requirement that matches your organization’s security requirements for valid passwords. For example, you can specify that a password must be a certain character length. Select Add a password requirement to add more items for subscribers when they change their password.
5. When you’re finished adding requirements, select **Save**.

6. Select **Save** again to save all your setting changes.
Allow Account Password to be Changed

- Enabled

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

Password must meet the following 4 requirements:

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

Subscriber experience when changing passwords

Tip:

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

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

Select View Password Requirements to display all the requirements you entered in Workspace Configuration.
Subscribers are automatically signed out of Workspace after changing their password and must sign in again with their new password.

**Configure custom banners**

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

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

1. From the Citrix Cloud menu, select **Workspace Configuration > Customize > Preferences > Custom banner > Configure**.
2. Enter the title and text of the message you want to display, and select the dates and times for displaying the banner to subscribers.
3. To view how your banner will appear to subscribers, select **Preview**.
4. When you’re finished, select **Save**.

**Configure a sign-in policy**

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

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

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

8. When you’re finished, select **Save**.

**Note**

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

January 26, 2022

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

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

Note:
You can’t use service continuity and fall back to StoreFront together. Choose the resiliency option that is best suited to your organization’s needs.

Site aggregation

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

For more information, visit Aggregate on-premises virtual apps and desktops in workspaces

Direct Workload Connection

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

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

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

Service continuity

Service continuity ensures that subscribers maintain access to critical apps and desktops through Citrix Workspace app if there’s a Citrix Cloud outage.
Citrix Workspace

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

**Fall back to StoreFront**

Fall back to StoreFront allows subscribers to temporarily switch to StoreFront during an outage. Fall back to StoreFront is an alternative to service continuity and is intended for organizations that still maintain at least one on-premises StoreFront within their Citrix deployment.

Fall back to StoreFront allows you to configure one or more StoreFront URLs to use if there's a disruption that prevents access to Citrix Cloud components. For more information, visit Fall back to StoreFront.

**Citrix Federated Authentication Service (FAS)**

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

Using FAS with Workspace has the following requirements:

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

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

**Aggregate on-premises virtual apps and desktops in workspaces**

January 12, 2022

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

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

**Supported environments**

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

- Virtual Apps and Desktops 7 1808 or later
- XenApp and XenDesktop 7.0 through 7.18
- XenApp 6.5

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

**Important:**

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

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

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

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

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

**Task overview**

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

1. Discover your site and select the resource location you want to use.
2. Detect the Active Directory domains in which your Cloud Connectors are installed.
3. Specify the connectivity that you want to use between Citrix Cloud and your site.
Citrix Workspace

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

For XenApp 6.5, Citrix Cloud also detects if there are any published applications assigned to local user accounts on XenApp servers. To use Citrix Workspace, application users must authenticate with Active Directory. Citrix Cloud provides a list of local user accounts detected so you can check that they can authenticate to Citrix Workspace.

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

Prerequisites

Cloud Connectors

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

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

- Meet the system requirements described in Cloud Connector Technical Details.
- Have no other Citrix components installed.
- Not be an Active Directory domain controller.
- Not be a machine that is critical to your resource location infrastructure.
- Be joined to your site domain. If users access your site’s applications in multiple domains, install at least two Cloud Connectors in each domain.
- Connect to a network that can contact your site.
- Connect to the Internet. For more information, see System and Connectivity Requirements.

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

Web proxy configuration

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

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

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

2. Import the list so that the Cloud Connector services can consume them. At the command prompt, type `netsh winhttp import proxy source=ie`.

3. From the **Services** console, restart all Citrix Cloud services on each machine hosting the Cloud Connector or restart each machine.

**Active Directory**

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

**Azure Active Directory configuration**

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

- For XenApp and XenDesktop 7.x and Virtual Apps and Desktops 7 1808, see **CTX236929**.
- For XenApp 6.5, see **Configuring the Citrix XML Service Port and Trust**.

**Important:**

If you use Azure Active Directory, Okta, SAML, or other federated identity provider with workspaces and site aggregation, users are prompted to authenticate to each application they launch.

FAS provides a single sign-on (SSO) experience for launching resources using federated authentication. To enable SSO for subscribers, register one or more FAS servers with the same resource location that you configured for adding your site.

**Active Directory trusts**

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

**Limitations:**

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

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

**Internal and external connectivity to workspace resources**

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

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

- Use your existing Citrix Gateway to handle the traffic between your on-premises site and Citrix Cloud. Your Citrix Gateway must be configured to use Cloud Connectors as the Secure Ticket Authority (STA) servers **before** you add your Site to Citrix Workspace. For instructions, see CTX232640.

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

**Note:**

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

**Credentials and ports for site discovery**

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

- You have Citrix administrator credentials with a minimum of **Read Only** permissions. During the site discovery process, Citrix Cloud prompts you to supply these credentials. Citrix Cloud doesn’t store these credentials or use them to change to your site.

- **XenApp 6.5 only:** Port 2513 on the XenApp server is accessible from the Cloud Connector machines in your environment. During the site discovery process, the Cloud Connectors contact
the Citrix XenApp Remoting Service on the XenApp server that you specify. This service listens on port 2513. If this port is blocked, Citrix Cloud can’t discover your XenApp 6.5 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 site credentials for security reasons, you can allow Citrix Cloud to discover your site without prompting for site credentials. Complete this task **before** you add your site to Citrix Workspace.

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

**Task 1: Discover site**

In this step, you provide the information that Citrix Cloud needs to locate your site and select your resource location. The resource location specifies the domain and connectivity option for all users who access your site. If you need to install Cloud Connectors in your site’s domain, you can do so now. If you already have Cloud Connectors installed, you can select them when prompted.

1. From the Citrix Cloud menu, navigate to **Workspace Configuration > Sites > Add Site.**
2. Select the type of on-premises site you want to add and continue.

   Citrix Cloud attempts to discover any resource locations and Cloud Connectors in your domain and displays a list for you to select from.

3. Perform one of the following actions:

   • If you have no Cloud Connectors installed in your site’s domain, select **Install Connector.** Citrix Cloud prompts you to download the Cloud Connector software and complete the installation wizard.
   • If you have Cloud Connectors installed, Citrix Cloud displays the connectors in the domains in which they were detected. Select the resource location you want to add to Citrix Workspace. This resource location becomes the default resource location.
   • If you have Cloud Connectors installed, but they aren’t displayed, select **Detect.**

4. Select the resource location and Cloud Connector pair that you want to use to discover your site.

5. In **Enter Server Address,** add the IP address or FQDN of a Controller in the site, and select **Discover**
Note:
If using an FQDN, you must have a DNS record that points to the Delivery Controller that you want to discover.

**XenApp 6.5 only:** Enter the port for the XML Server. If the XML Server port uses SSL, select **Use SSL**.
For XenApp and XenDesktop 7.x sites, Citrix Cloud automatically discovers the XML server port.

6. If prompted, enter the Citrix Administrator credentials for the site.

Citrix Cloud tests connectivity to verify that your site is reachable. Discovery might take a few minutes to complete, depending on the type and size of the site.

7. If a success message appears indicating that the site has been successfully discovered, select **Continue**.

**Task 2: Verify Active Directory Connection**

In **Verify Active Directory Connection**, Citrix Cloud displays the domains used with your site and whether there are Cloud Connectors installed in those domains.

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 you only have one Cloud Connector in your domain, you have two options:

- Install more Cloud Connectors by selecting **Install Connector**.
- Continue without installing more Cloud Connectors by selecting **I understand that high availability requires having two connectors installed in each domain**.

**XenApp 6.5:** If there are local user accounts assigned to published applications, they must be assigned to applications using their Active Directory account. Otherwise, users 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.

If you have local users assigned to applications in your site, select **Download user list (.csv)**.

After verifying your Active Directory connection, select **Continue**.

**Task 3: Configure connectivity**

In this step, you specify whether you want to allow external or internal-only user access to your site through Citrix Workspace. Internal connectivity requires your users to be on the same network as your
site and VDAs that host your published resources. For external connectivity, you can use your existing on-premises Citrix Gateway or you can use the cloud-hosted Citrix Gateway service.

Select one of the following options in **Select connectivity type > Configure Connectivity**:

- **Add Existing Gateway**: Select this option to use your existing Citrix Gateway to provide external access.
- **Citrix Gateway service**: Select this option to activate a service trial or to use your existing subscription with your site.
- **Internal Only**: Select this option if no other configuration is needed.

If **Add Existing Gateway** is selected, perform the following actions:

1. Select **Edit** and enter the public URL of the Citrix Gateway.
2. Verify that Citrix Gateway is configured to use your Cloud Connectors as the STA servers, described in CTX232640.
3. Select **Test STA** and then, when the test is successful, **Continue**. If the test isn’t successful, refer to CTX232517 for troubleshooting.

If **Citrix Gateway service** is selected, but the service isn’t enabled for your Citrix Cloud account as a service trial or as a purchase, you can select **Start a 60-day trial**. Citrix Cloud enables the service as a trial for you. If the service was enabled at an earlier time, Citrix Cloud detects the service and displays any remaining trial days.

After completing the preceding tasks, select **Continue**.

**Task 4: Confirm site aggregation**

In this step, you confirm site aggregation, which involves reviewing the XML port, XML servers, Active Directory domains, and the connectivity type you chose earlier.

Citrix Cloud displays up to five XML servers it can connect to. If you have more than one XML server in your site but only one is shown, Citrix Cloud displays an alert. To troubleshoot this issue, refer to CTX232516.

1. In **Confirm Site Aggregation**, review the XML port, XML servers, Active Directory domains, and the connectivity type you chose earlier.
2. Select **Save and Finish**. The **Sites** page displays your newly added site.

If you want to specify different XML servers, you can then edit your site to change these values after you select **Save and Finish**.

**Task 5: Manage service integrations**

After adding your first site, you must enable the **Service Integration** for Virtual Apps and Desktops on-premises sites, which is disabled by default. Subscribers can’t see resources from the site until you
enable it.

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

Change your site configuration

Rediscover your site

If you add Delivery Controllers to your site or change XML ports, you can verify that your site is still reachable in Citrix Workspace with a rediscovery process.

1. Navigate to Workspace Configuration > Sites, select the ellipsis for the site you want to update, and then select Edit Site.
2. In Server Address, type the IP address or FQDN of a Delivery Controller in your site and select Rediscover.

Add or modify XML servers

When you add a site to Citrix Workspace, Citrix Cloud automatically detects XML servers in your site and displays up to five XML servers in your configuration. You can add and remove XML servers as needed from your site configuration up to the display limit of five XML servers.

To add an XML server

1. Navigate to Workspace Configuration > Sites, select the ellipsis for the site you want to update and select Edit Site.
2. In the XML Servers section, enter the XML server port and select Use SSL if needed.
3. Select a connectivity method:
   - Load balanced: This option allows Citrix Cloud to pick a random XML server from the list.
   - Failover: This option allows Citrix Cloud to use the listed XML servers in the order that they appear in the list. Only the first XML service in the list is used for launch unless it becomes unavailable, then the second server is used. You can reorder the list by dragging and dropping each server.
4. Select Save Changes.

If you experience an error when adding an XML server, refer to CTX232516 for troubleshooting steps.
Add IP ranges for different connectivity options

If you haveVDAs or session hosts in different subnets, you can specify IP ranges with a different connectivity type for each one. Each IP range can also have a different resource location associated with it. For example, you might have one IP range for machines in the EU where users connect internally, one IP range for machines in the EU where users connect through your Citrix Gateway, and one IP range for machines in the US where users connect through the Citrix Gateway service.

1. Navigate to Workspace Configuration > Sites, select the ellipsis button for the site you want to update, and select Edit Site.
2. In the Connectivity section, select Add an IP range with a different connectivity option and enter an IP range in CIDR format.

To create a resource location for your IP range:

1. Select Add a new Resource Location and enter a user-friendly name.
2. In Select your connectivity, select whether you want to provide internal-only access or allow external access using your Citrix Gateway or the Citrix Gateway service.
3. If you choose a resource location with only one Cloud Connector installed, select I understand that high availability requires having two connectors are installed in a resource location.
4. Select Add.

Add more Active Directory domains

If you install Cloud Connectors in more domains with Active Directory users in your site, you can check they’re added to your site configuration in Citrix Workspace.

1. Navigate to Workspace Configuration > Sites, select the ellipsis for the site you want to update, and then select Edit Site.

Disable Sites

If you no longer want to make your on-premises site available to users in Citrix Workspace, you can disable it. You can disable an individual on-premises site or all on-premises sites you’ve added to Citrix Workspace.

When sites are disabled, users can’t access the on-premises applications in those sites through Citrix Workspace. However, the configuration for those sites is preserved. If you re-enable a site later on, the site's default resource location, domain, XML server, and connectivity settings are kept.
To disable an on-premises site

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

To disable all on-premises sites

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

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

Delete a site from Citrix Workspace

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

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

Optimize connectivity to workspaces with Direct Workload Connection

February 16, 2022

With Direct Workload Connection in Citrix Cloud, you can optimize internal traffic to the apps and desktops in workspaces to make HDX sessions faster. Ordinarily, users on both internal and external networks connect to VDAs through an external gateway. Direct Workload Connection allows internal users to bypass the gateway and connect to the VDAs directly, reducing latency for internal network traffic.

To set up Direct Workload Connection, you need network locations that correspond to the VDAs in your environment with the Network Location Service (NLS). You have two options for configuring network locations:

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

Network locations correspond to the public IP ranges of the networks that your internal users connect from, such as your office or branch locations. Citrix Cloud uses public IP addresses to determine
whether networks from which virtual apps or desktops are launched in Workspace are internal or external to the company network. If a subscriber connects from the internal network, Citrix Cloud routes the connection directly to the VDA, bypassing Citrix Gateway. If a subscriber connects externally, Citrix Cloud routes them through Citrix Gateway, then redirects the subscriber through the Citrix Cloud Connector to the VDA in the internal network.

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

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

**Requirements**

**Network requirements**

- Corporate network and guest Wi-Fi networks must have separate public IP addresses. If your corporate and guest networks share public IP addresses, users on the guest network can’t launch Virtual Apps and Desktops sessions.
- Use the public IP address ranges of the networks that your internal users connect from. Internal users on these networks must have a direct connection to the VDAs. Otherwise, launches of virtual resources will fail as Workspace tries to route internal users directly to the VDA, which isn’t possible.

**TLS requirements**

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

```
```

**Workspace requirements**

- You have a workspace configured in Citrix Cloud.
- The Virtual Apps and Desktops service is enabled in **Workspace Configuration > Service Integrations**.
- You’re using on-premises VDAs to deliver virtual resources to workspace subscribers.
Enable TLS for Workspace app for HTML5 connections

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

Citrix Cloud network location configuration

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

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

2. Select the **Add network location** button in the top right-hand corner.
3. Enter a network location name, public IP address range for the location, and location tags.

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

Modify or remove network locations

1. In the Citrix Cloud console, navigate to **Network Locations** from the main menu.
2. Select the ellipses next to the network location that you want to modify or remove and then either:
   - Select **Edit** to modify a network location and then **Save** your changes to see them in the network locations page; or
Citrix Workspace

- Select **Delete** to remove a network location. You’re asked to confirm this decision before the network location is deleted. You can’t undo this action.

**PowerShell network location configuration**

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

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

**Download the PowerShell module**

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

2. Press **ALT** while clicking the **Raw** button.
3. Select a location on your computer and click **Save**.
Citrix Workspace

**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**

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.

   ![Identity and Access Management](image)

   Secure Clients are used to interact with Citrix Cloud APIs. [Learn more about the APIs](https://examplecorp).

   To use a secure client in a silent Cloud Connector install or to access Citrix Cloud APIs, use `examplecorp` in the customer ID parameter.

   ![Name your Secure Client](image)

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

1. Open a PowerShell command window and navigate to the same directory where you saved the PowerShell module.

2. Import the module: `Import-Module .\nls.psm1 -Force`

3. Set the required variables with your secure client information from Create a secure client:
   - `$clientId = "YourSecureClientID"
   - `$customer = "YourCustomerID"
   - `$clientSecret = "YourSecureClientSecret"

4. Connect to the Network Location Service with your secure client credentials:

   ```powershell
   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:

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

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

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

Important:

When using the `New-NLSSite` command, include at least one value for each parameter. If you run this command without any command-line arguments, PowerShell prompts you to enter appropriate values for each parameter, one at a time. When entering values for the `tags` parameter, press ENTER after entering each tag value. When you’re finished entering tags, press ENTER again to proceed to the next parameter. The `internal` property is a mandatory boolean property with possible values: $True or $False that maps to the UI via Powershell. For example, (UI)Network Internal → (PowerShell)-internal
When the network location is created successfully, the command window displays the details of the network location.

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

**Verify that internal launches are routed correctly**

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

- View VDA connections through Virtual Apps and Desktops console.
- Use ICA file logging to verify the correct addressing of the client connection.

**Virtual Apps and Desktops service console**

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

**ICA file logging**

Enable ICA file logging on the client computer as described in To enable logging of the launch.ica file. After launching sessions, examine the **Address** and **SSLProxyHost** entries in the log file.

For direct VDA connections, the **Address** property contains the VDA’s IP address and port and the **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**

To change an existing network location:

1. From a PowerShell command window, list all existing network locations: `Get-NLSSite`
2. To modify the IP range for a specific network location, type  
   
   ```powershell
   (Get-NLSSite)[N] | Set-NLSSite -ipv4Ranges @("1.2.3.4/32","4.3.2.1/32")
   ```

   where `[N]` is the number corresponding to the location in the list (starting with zero) and ”1.2.3.4/32”, ”4.3.2.1/32” are the comma-separated IP ranges you want to use. For example, to modify the first listed location, you type the following command:
(Get-NLSSite[0] | Set-NLSSite -ipv4Ranges @"98.0.0.1/32", "141.43.0.0/24")

Remove network locations

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

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

Example script

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

```
1 Import-Module .\nls.psm1 -Force
2
3 $clientId = "XXXX" #Replace with your clientId
4 $clientSecret = "YYY"  #Replace with your clientSecret
5 $customer = "CCCCCC" #Replace with your customerId
6
7 # Connect to Network Location Service
8 Connect-NLS -clientId $clientId -clientSecret $clientSecret -customer $customer
9
10 # Create a new Network Location Service Site (Replace with details corresponding to your branch locations)
11 New-NLSSite -name "New York" -tags @("EastCoast") -ipv4Ranges @("1.2.3.0/24") -longitude -40.7128 -latitude -74.0060 -internal $True
12
13 # Get the existing Network Location Service Sites (optional)
14 Get-NLSSite
15
16 # Update the IP Address ranges of your first Network Location Service Site (optional)
17 $s = (Get-NLSSite)[0]
```
Troubleshooting

VDA launch failures

If VDA sessions are failing to launch, verify you are using public IP address ranges from the correct network. When configuring your network locations, you must use the public IP address ranges of the network where your internal users are connecting from. For more information, see Requirements in this article.

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

Internal VDA launches still routed through the gateway

If VDA sessions launched internally are still being routed through the gateway as if they were external sessions, verify you are using the correct IP address ranges for the networks where your internal users are connecting from. These are generally the public IP address ranges that correspond to the networks where your VDAs reside, although your users might access the VDAs through a VPN. Do not use the local IP addresses of the VDAs. For more information, see Requirements in this article.

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

Errors when running PowerShell cmdlets on non-Windows platforms

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

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

March 2, 2022

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

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

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

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

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

Service continuity is supported for double hop scenarios when Citrix Workspace app is installed on a virtual desktop.

For an in-depth technical article about Citrix Cloud resiliency features, including service continuity, see [Citrix Cloud Resiliency](#).
Note:
The deprecated Citrix Virtual Apps and Desktops feature called “connection leasing” resembles Workspace connection leases in that it improved connection resiliency during outages. Otherwise, that deprecated feature is unrelated to service continuity.

User device setup

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

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

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

Downloading Workspace connection leases might take up to 15 minutes for first-time sign-in.

User experience during an outage

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

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

For some outages, users continue accessing their virtual apps and desktops with no change to their user experience. For other outages, user might see a change in how Workspace appears or be prompted to take some action.

This table summarizes how service continuity helps users access apps and desktops during different types of outages.
<table>
<thead>
<tr>
<th>Where the outage occurs</th>
<th>How service continuity maintains user access</th>
<th>User experience during outage</th>
</tr>
</thead>
<tbody>
<tr>
<td>Citrix Workspace service</td>
<td>Citrix Workspace app enumerates apps and desktops based on local cache on the user device.</td>
<td>Icons for unavailable apps and desktops appear dimmed. Users can still access apps and desktops that have undimmed icons. After clicking an undimmed icon, users might be prompted to reenter their credentials at the VDA. To regain access to all their apps and desktops, users can try to establish their connection to Workspace by clicking the “Reconnect to Workspace” link.</td>
</tr>
<tr>
<td>Identity provider</td>
<td>Citrix Workspace app and desktops based on local cache on the user device.</td>
<td>Users might be unable to sign in to Workspace. Users click the “Use Workspace offline” link to access some apps and desktops in an experience identical to a Workspace service outage.</td>
</tr>
<tr>
<td>Citrix Cloud Broker Service</td>
<td>The High Availability Service in the Cloud Connector takes over brokering. All VDAs that were registered with the Cloud Broker Service register with the High Availability Service.</td>
<td>Some users might be unable to access virtual resources while VDAs register with the High Availability Service. Existing sessions aren’t affected. No user action needed.</td>
</tr>
<tr>
<td>Secure Ticket Authority</td>
<td>Workspace connection leases provide access to virtual resources when ICA files can’t.</td>
<td>Sessions launches might take a few seconds longer. No user action needed.</td>
</tr>
<tr>
<td>Citrix Gateway service</td>
<td>Network traffic fails over to the closest healthy Citrix Gateway service point of presence (POP).</td>
<td>Existing sessions might take a few seconds to reconnect. No user action needed.</td>
</tr>
</tbody>
</table>
## Citrix Workspace

<table>
<thead>
<tr>
<th>Where the outage occurs</th>
<th>How service continuity maintains user access</th>
<th>User experience during outage</th>
</tr>
</thead>
<tbody>
<tr>
<td>Internet connection on the LAN</td>
<td>Citrix Workspace app enumerates apps and desktops based on local cache on the user device. If a user has a direct network connection to the resource location, Citrix Workspace app bypasses the Citrix Gateway service when the user clicks undimmed icons. Citrix Workspace app contacts the Cloud Connector over TCP 2598 and contacts VDAs over TCP 2598 or UDP 2598.</td>
<td>Icons for unavailable apps and desktops appear dimmed. Users can still access apps and desktops that have undimmed icons. After clicking an undimmed icon, users might be prompted to reenter their credentials at the VDA. To regain access to all their apps and desktops, users can try to establish their connection to Workspace by clicking the “Reconnect to Workspace” link.</td>
</tr>
</tbody>
</table>

During a Citrix Workspace outage, users see this message at the top of the Citrix Workspace home page: “Unable to connect to some of your resources. Some virtual apps and desktop may still be available.” Users see apps and desktops that they can connect to during the outage. If the app or desktop isn’t available, the icon appears dimmed.
To access available resources during an outage, users select a resource icon that isn’t dimmed. If prompted, the user then reenters their AD credentials at the VDA before accessing resources.

During an outage in the identity provider for workspace authentication, users might be unable to sign in to Citrix Workspace through the Workspace sign-in page. After 40 seconds, this message appears at the top of the Citrix Workspace home page.
Afterward, the Citrix Workspace home page appears. Users then access resources as they would during a Citrix Workspace outage.

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

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

Depending on how Citrix Workspace app and VDAs are configured, during an outage the VDA might prompt users to enter their credentials into the Windows Logon user interface. If this prompt occurs, users enter their Active Directory (AD) credentials or smart card PIN to access the app or desktop. This step is required when user credentials aren’t passed through during outages. Before accessing an app or desktop, users must reauthenticate to the VDA.

Users can access resources without entering their AD credentials if:

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

When enabled, single sign-on remembers your credentials for this device, so that you can connect to other Citrix applications without having to sign in each time. You should do this only if your IT administrator has instructed you to. This will take effect the next time you log on to this device.

- Enable single sign-on

For more information on configuring single sign-on, please see article CTX133982 at citrix.com/support.

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

  Note

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

- Session sharing is enabled. Users can access apps or desktops hosted on the same VDA after they provide their credentials for one resource on that VDA. Session sharing is configured for the application group containing the resource on the VDA. For information about configuring application groups, see Create application groups.

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

Requirements and limitations

Site requirements

- Supported in all editions of the Citrix Virtual Apps and Desktops service and Citrix Virtual Apps and Desktops Standard for Azure, when using Workspace Experience.

- Not supported for Citrix Workspace with site aggregation to on-premises Virtual Apps and Desktops.

- Not supported for on-premises Citrix Gateway.
User device requirements

- Citrix Workspace app 2106 for Windows, Citrix Workspace app 2106 for Mac, Citrix Workspace app 2106 for Linux, or Citrix Workspace app for Android 22.2.0 at a minimum. Citrix Workspace app for iOS 22.2.5 is available for technical preview.

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

- For users who access their apps and desktops using browsers:
  - Google Chrome or Microsoft Edge.
  - Citrix Workspace app 2109 for Windows at a minimum. Supported with Google Chrome and Microsoft Edge.
  - Citrix Workspace app for Mac version 2112 at a minimum. Supported with Google Chrome.
  
  See Service continuity in browser.

- Only one user per device is supported. Kiosk or “hot desk” user devices aren’t supported.

Supported workspace authentication methods

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

Authentication limitations

- Single sign-on with Citrix Federated Authentication Service (FAS) isn’t supported. Users enter their AD credentials into the Windows Logon user interface on the VDA.
- Single sign-on to VDA isn’t supported.
- Local mapped accounts aren’t supported.
- VDAs joined to Azure AD aren’t supported. All VDAs must be joined to an AD domain.

Citrix Cloud Connector scale and size

- 4 vCPU or more
- 4 GB memory or more
Citrix Cloud Connector connectivity

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

Workspace app network connectivity

If you configure connection to your resource location from outside your LAN, the Workspace app on user devices must be able to reach the Citrix Gateway Service FQDN, https://*.g.nssvc.net. Ensure that your firewall is configured to allow outgoing traffic to https://global-s.g.nssvc.net:433, so that user devices can connect to the Citrix Gateway Service at all times.

Connectivity optimization limitations

Advanced Endpoint Analysis (EPA) isn’t supported.

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

VDA requirements and limitations

- VDA 7.15 LTSR or any current release that hasn’t reached end of life are supported.
- VDAs joined to Azure AD aren’t supported. All VDAs must be joined to an AD domain.
- VDAs must be online for users to access VDA resources during an outage. VDA resources aren’t available when the VDA is affected by outages in:
  - AWS
  - Azure
  - Cloud Delivery Controller, unless Autoscale is enabled for the delivery group delivering the resource

Note:

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

- VDA workloads supported during outages:
  - Hosted shared apps and desktops
  - Random non-persistent desktops (pooled VDI desktop) with power management
  - Static non-persistent desktops
  - Static persistent desktops, including Remote PC Access
Citrix Workspace

Note:
Assign on first use isn’t support during outages.

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

App protection limitations

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

For more information about app protection policies, see App protection.

Local keyboard mapping requirements and limitations

The Windows Logon user interface that prompts users to reauthenticate on the VDA does not support local keyboard language mapping. To allow users to reauthenticate during an outage if they have local keyboard language mapping on their devices, preload the keyboard layouts these users require.

Warning:
Editing the registry incorrectly can cause serious problems that might require you to reinstall your operating system. Citrix can’t guarantee that problems resulting from the incorrect use of the Registry Editor can be solved. Use the Registry Editor at your own risk. Be sure to back up the registry before you edit it.

Edit this registry key in the VDA image:

HKEY_USERS\.DEFAULT\Keyboard Layout\Preload

The corresponding language pack in the virtual desktop image must be installed.

For a list of keyboard identifiers associated with keyboard languages, see Keyboard Identifiers and Input Method Editors for Windows.

Configure resource location network connectivity for service continuity

You can configure your resource location to accept connections from inside your LAN, outside your LAN, or both.

Configure for connections inside your LAN

1. From the Citrix Cloud menu, go to Workspace Configuration > Access.
2. Select **Configure Connectivity**.
3. Select **Internal Only** as your connectivity type.
4. Click **Save**.

Configure your Citrix Cloud Connector and VDA firewalls to accept connections over Common Gateway Protocol (CGP) TCP port 2598. This configuration is the default setting.

**Configure for connections from outside your LAN**

1. From the Citrix Cloud menu, go to **Workspace Configuration > Access**.
2. Select **Configure Connectivity**.
3. Select **Gateway Service** as your connectivity type.
4. Click **Save**.

**Configure for connections both from outside and inside your LAN**

Run this PowerShell command:

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

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

This command allows direct connections to the Citrix Cloud Connector FQDN over TCP 2598 during outages. If that connection fails Gateway Service is used as fallback. Allow internal users to bypass the gateway and connect directly to the resource location reduces latency internal network traffic.

**Note:**

This PowerShell command is similar to Direct Workload Connection in that it optimizes connectivity to workspaces by allowing internal users to bypass the gateway and connect to VDAs directly. When service continuity is enabled, Direct Workload Connection is not available during outages.

**Configure service continuity**

To enable service continuity for your site:

1. From the Citrix Cloud menu, go to **Workspace Configuration > Service continuity**.
2. Set **Connection leasing for the Workspace** to **Enable**.
3. Set **Connection lease period** to the number of days a Workspace connection lease can be used to maintain a connection. The Workspace connection lease period applies to all Workspace connection leases through your site. The Workspace connection lease period starts the first time a user signs in to the Citrix Cloud Workspace store. Workspace connection leases are refreshed each time the user signs in, up to once a day. The Workspace connection lease period can be from one day to 30 days. The default is seven days.

4. Click **Save**.

When you enable service continuity, it is enabled for all delivery groups in your site. To disable service continuity for a delivery group, use the following PowerShell command:

```
Set-BrokerDesktopGroup -name <deliverygroup> -ResourceLeasingEnabled $false
```

Replace `<deliverygroup>` with the name of the delivery group.

By default, Workspace connection leases are deleted from the user device if the user signs out of Citrix Workspace during an outage. If you want Workspace connection leases to remain on user devices after users sign out, use the following PowerShell command:

```
Set-BrokerSite -DeleteResourceLeasesOnLogOff $false
```

**Note:**

Workspace connection leases can’t be set to remain on user devices after users sign out for users connecting with Citrix Workspace app for Mac. Citrix Workspace for Mac is unable to read the value of the `DeleteResourceLeaseOnLogOff` property.

**How service continuity works**

If there’s no outage, users access virtual apps and desktops using ICA files. Citrix Workspace generates a unique ICA file each time a user selects a virtual app or desktop icon. Each ICA file contains a Secure Ticket Authority (STA) ticket and a logon ticket that can be redeemed only once to gain authorized access to virtual resources. The tickets in each ICA file expire after about 90 seconds. After the ticket in an ICA file is used or expires, the user needs another ICA file from Citrix Workspace to access resources. When service continuity isn’t enabled, outages can prevent users from accessing resources if Citrix Workspace can’t generate an ICA file.
Citrix Workspace generates ICA files when users launch virtual apps and desktops regardless of whether service continuity is enabled. When service continuity is enabled, Citrix Workspace also generates the unique set of files that make up a Workspace connection lease. Unlike ICA files, Workspace connection lease files are generated when the user signs into Citrix Workspace, not when the user launches the resource. When a user signs in to Citrix Workspace, connection lease files are generated for every resource published to that user. Workspace connection leases contain information that gives the user access to virtual resources. If an outage prevents a user from signing in to Citrix Workspace or accessing resources using an ICA file, the connection lease provides authorized access to the resource.

### How sessions launch during outages

When users click an icon for an app or desktop during an outage, the Citrix Workspace app finds the corresponding Workspace connection lease on the user device. Citrix Workspace app then opens a connection. If connectivity to the resource location that hosts the app or desktop is configured to accept connections from outside your LAN, a connection opens to Citrix Gateway Service. If you configure connectivity to the resource location that hosts the app or desktop to accept connections from inside your LAN only, a connection opens to the Cloud Connector.

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

Users who are connected when an outage occurs can continue working uninterrupted. Reconnections and new connections experience minimal connection delays. This functionality is similar to Local Host Cache, but does not require an on-premises StoreFront.

When a user launches a session during an outage, this window appears indicating that Workspace connection leases were used for the session launch:

![Starting...](image)

After the user has finished signing into the session, these properties appear in the Workspace Connection Center:
The launch mode property provides information about the Workspace connection leases used to launch the session.

On devices running Citrix Workspace app for Mac, Citrix Viewer displays information showing that Workspace connection leases were used for the session launch:
What makes it secure

All sensitive information in the Workspace connection lease files is encrypted with the AES-256 cipher. Workspace connection leases are bound to a public/private key pair uniquely associated with the specific client device and can’t be used on a different device. A built-in cryptographic mechanism enforces use of the unique key pair on each device.

Workspace connection leases are stored on the user device in AppData\Local\Citrix\SelfService\ConnectionLeases.

The security architecture of service continuity is built on public-key cryptography, similarly to a public key infrastructure (PKI), but without certificate chains and certificate authorities. Instead, all the components establish transitive trust by relying on a new Citrix Cloud service called the root of trust that acts like a certificate authority.

Block connection leases

If a user device is lost or stolen, or a user account is closed or compromised, you can block Workspace connection leases. When you block Workspace connection leases associated with a user, the user can’t connect to resources. Citrix Cloud no longer generates or synchronizes Workspace connection leases for the user.

When you block Workspace connection leases associated with a user account, you block connections to that account on all devices associated with it. You can block Workspace connection leases for a user or for all users in a user group.

To revoke Workspace connection leases for a single user or user group, use this PowerShell command:

```
Set-BrokerConnectionLeaseRevocationDate -Name username -LeaseRevocationDays Days
```
Citrix Workspace

Replace `username` with the user associated with the account you want to block from connecting. Replace `username` with a user group to block connection from all accounts in the user group. Replace `Days` with the number of days connections are blocked.

For example, to block connections for xd.local/user1 for the next 7 days, type:

```powershell
Set-BrokerConnectionLeaseRevocationDate -Name xd.local/user1 -LeaseRevocationDays 7
```

To view the time period for which Workspace connection leases are revoked, use this PowerShell command:

```powershell
Get-BrokerConnectionLeaseRevocationDate -Name username
```

Replace `username` with the user or user group you want to view the time period for.

For example, to view the time period for which Workspace connection leases are revoked for xd.local/user1, type:

```powershell
Get-BrokerConnectionLeaseRevocationDate -Name xd.local/user2
```

This information appears:

```powershell
1 FullName :                     
2 Name : XD\user2                
3 UPN :                         
4 Sid : S-1-5-21-nnnnnn         
5 LeaseRevocationDays : 2        
6 LeaseRevocationDateTimeInUtc : 2020-12-17T17:34:25Z 
7 LastUpdateTimeInUtc : 2020-12-19T17:34:25Z 
```

From this output, you can see that user xd.local/user2 has Workspace connection leases revoked for two days, from December 17, 2020, through December 19, 2020, at 17:34:25 UTC on each day.

To allow a user account that has Workspace connection leases revoked to receive connection again, remove the block using this PowerShell command:

```powershell
Remove-BrokerConnectionLeaseRevocationDate -Name username
```

Replace `username` with the blocked user or user group you want to receive connection. To allow all blocked user account to receive connections, leave out the `Name` option.
Double hop scenarios

Service continuity can allow users to access virtual resources during outages in double hop scenarios if they’re signed in to Citrix Workspace before the outage occurs. In a double hop scenario, a physical user device connects to a virtual desktop that has Citrix Workspace app installed. The virtual desktop then connects to another virtual resource.

In the double hop scenario, service continuity can allow users to access virtual resources during an outage regardless of the type of virtual desktop. If the virtual desktop retains user changes, service continuity can also provide access to virtual resources during outages that occur while the user isn’t signed in.

Service continuity treats the physical user device and the virtual device in a double hop scenario as individual client endpoints. Each device has its own set of Workspace connection leases. When a user signs in to Citrix Workspace on a physical device, Workspace connection lease files are downloaded and saved to the user profile on the physical device. The user then accesses a virtual desktop and signs in to Citrix Workspace on the virtual desktop. At this point, a different set of Workspace connection leases is downloaded and saved the user profile on the virtual desktop. Workspace connection lease files are associated with the device they’re downloaded to. Workspace connection lease files can’t be copied to another device and reused, even by the same user. Thus, service continuity can’t provide access to resources during outages that occur after the session ends if the virtual desktop discards changes made during a user session. For this type of virtual desktop, Workspace connection leases are among the changes discarded.

Here’s how service continuity works in double hop scenarios with each type of supported virtual desktop.

<table>
<thead>
<tr>
<th>For double hops that include…</th>
<th>Service continuity can provide access to virtual resources during outages…</th>
</tr>
</thead>
<tbody>
<tr>
<td>Hosted shared desktops</td>
<td>If the outage occurs while the user is signed in to the virtual desktop.</td>
</tr>
<tr>
<td>Random non-persistent desktops (pooled VDI desktop)</td>
<td>If the outage occurs while the user is signed in to the virtual desktop.</td>
</tr>
<tr>
<td>Static non-persistent desktops</td>
<td>If the virtual desktop hasn’t restarted since the user last logged in.</td>
</tr>
<tr>
<td>Static persistent desktops</td>
<td>Anytime an outage occurs.</td>
</tr>
</tbody>
</table>

VDA management during outages

Service continuity uses the Local Host Cache function within the Citrix Cloud Connector. Local Host Cache allows connection brokering to continue on a site when the connection between the Cloud
Delivery Controller and the Cloud Connector fails. Because service continuity relies on Local Host Cache, it shares some limitations with Local Host Cache.

**Note:**

Although service continuity uses Local Host Cache within the Cloud Connector, unlike Local Host Cache, service continuity isn’t supported with on-premises StoreFront.

**Power management of VDAs during outages**

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

- If your site uses Citrix Hypervisor or vSphere: The Cloud Connector can perform power management operations, including the Pooled VDI case, during an outage.
- If your site uses any other hypervisor: During an outage, all machines are in the unknown power state and no power operations can be issued. However, VMs on the host that are powered-on can be used for connection requests.

By default, power-managed desktop VDAs in pooled delivery groups that have the **Shutdown-DesktopsAfterUse** property enabled are placed into maintenance mode when an outage in the Citrix-managed broker occurs. You can change this setting to allow those desktops to be used during an outage. However, power management is only available during an outage if you’re using Autoscale with Citrix Hypervisor or vSphere. If those desktops are used during on outage, they might contain data from the previous user because they haven’t been restarted.

Power management resumes when normal operations resume after an outage.

**Machine assignment and automatic enrollment**

An assigned machine can be used only if the assignment occurred during normal operations. New assignments cannot be made during an outage.

Automatic enrollment and configuration of Remote PC Access machines isn’t possible. However, machines that were enrolled and configured during normal operation are usable.

**VDA resources in different zones**

Server-hosted applications and desktop users might use more sessions than their configured session limits, if the resources are in different zones.

Unlike Local Host Cache, service continuity can launch apps and desktops from registered VDAs in different zones, providing the resource is published in more than one zone. Citrix Workspace app
Citrix Workspace

might take longer to find a healthy zone as it cycles sequentially through all the zones in the Workspace connection lease.

**Monitoring and troubleshooting**

Service continuity performs two main actions:

- Download Workspace connection leases to the user device. Workspace connection leases are generated and synced with the Citrix Workspace app.
- Launch virtual desktops and apps using Workspace connection leases.

**Troubleshooting downloading Workspace connection leases**

You can view Workspace connection leases at this location on the user device.

On Windows devices:

\[C:\Users\Username\AppData\Local\Citrix\SelfService\ConnectionLeases\Store GUID\User GUID\leases\]

**Username** is the user name.

**Store GUID** is the global unique identifier of the Workspace store.

**User GUID** is the global unique identifier of the user.

On Mac devices:

\[\$HOME/Library/Application Support/Citrix Receiver/CLSyncRoot\]

For example, open \[/Users/luca/Library/Application Support/Citrix Receiver/CLSyncRoot\]

On Linux:

\[\$HOME/.ICAClient/cache/ConnectionLease\]

For example, open \[/home/user1/.ICAClient/cache/ConnectionLease\]

Workspace connection leases are generated when the Citrix Workspace app connects to the Workspace store. View registry key values on the user device to determine whether the Citrix Workspace app has successfully contacted the Workspace connection lease service in Citrix Cloud.

Open regedit on the user device and view this key:

\[HKCU\Software\Citrix\Dazzle\Sites\store-xxxx\]

If these values appear in the registry key, the Citrix Workspace app contacted or attempted to contact the Workspace connection lease service:

- leaseLastCallHomeTime
Citrix Workspace

- **leaseLastSyncStatus**

If the Citrix Workspace app tried unsuccessfully to contact the Workspace connection lease service, \texttt{leaseLastCallHomeTime} shows an error with an invalid time stamp:

\texttt{leaseLastCallHomeTime REG_SZ 1/1/0001 12:00:00 AM}

If \texttt{leaseLastCallHomeTime} is uninitialized, the Citrix Workspace app never attempted to contact the Workspace connection lease service. To resolve this issue, remove the account from the Citrix Workspace app and add it again.

**Citrix Workspace app error codes for Workspace connection leases**

When a service continuity error occurs on the user device, an error code appears in the error message. Common errors include:

<table>
<thead>
<tr>
<th>Error code</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>3000</td>
<td>No connection lease files present</td>
</tr>
<tr>
<td>3002</td>
<td>Connection lease cannot be read or found</td>
</tr>
<tr>
<td>3003</td>
<td>No resource location found</td>
</tr>
<tr>
<td>3004</td>
<td>Connection details missing in the leases</td>
</tr>
<tr>
<td>3005</td>
<td>ICA file is empty</td>
</tr>
<tr>
<td>3006</td>
<td>Connection lease expired. Log back into Workspace.</td>
</tr>
<tr>
<td>3007</td>
<td>Connection lease is invalid</td>
</tr>
<tr>
<td>3008</td>
<td>Connection lease validation result: empty</td>
</tr>
<tr>
<td>3009</td>
<td>Connection lease validation result: invalid</td>
</tr>
<tr>
<td>3010</td>
<td>Parameter missing</td>
</tr>
<tr>
<td>3020</td>
<td>Connection lease validation failed</td>
</tr>
<tr>
<td>3021</td>
<td>No resource location found where the app is published</td>
</tr>
<tr>
<td>3022</td>
<td>Connection lease validation result: deny</td>
</tr>
<tr>
<td>3023</td>
<td>Citrix Workspace app timed out</td>
</tr>
</tbody>
</table>
Service continuity in browser

Extensions for Google Chrome and Microsoft Edge make service continuity available to Windows users who access their apps and desktops using those browsers. The extensions are called a Citrix Workspace Web extension and are available at the [Chrome web store](https://chrome.google.com/webstore) and the [Microsoft Edge Add-on website](https://microsoft.com/store). These browser extensions require a native Citrix Workspace app on the user device to support service continuity. These versions are supported:

- Citrix Workspace app 2109 for Windows at a minimum. Supported with Google Chrome and Microsoft Edge.
- Citrix Workspace app for Mac version 2112 at a minimum. Supported with Google Chrome.

Citrix Workspace app for Windows (Store) is not supported.

The native Workspace app communicates with the Citrix Workspace Web extension using the native messaging host protocol for browser extensions. Together, the native Workspace app and the Workspace Web extension use Workspace connection leases to give browser users access to their apps and desktops during outages.

This video shows how to install and use service continuity in browser.

This is an embedded video. Click the link to watch the video

User device setup for browser users

To use service continuity in a browser, users must perform the following steps on their devices:

1. Download and install a version of Citrix Workspace app that is supported for browser users.
2. Download and install the Citrix Workspace Web extension for Chrome or Edge.

Browser user experience

When users click their apps or desktops, the app or desktop opens without users being prompted to open the **Citrix Workspace launcher**.

Browser user experience during outages

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

If an outage occurs while the user is logged in to Workspace through a browser, this message appears near the top of the browser window:
Users can access apps and desktops that are available offline by clicking any icon that is not dimmed. Users can also try to get back online by clicking **Reconnect to Workspace**.

When an outage prevents users from logging in to Workspace through a browser, the user is prompted work offline or try logging in again. To access available apps and desktops offline, users click **Use Workspace Offline**.

If an outage prevents users from logging in to the Workspace after navigating to the Workspace URL, the window appears after a specified timeout interval. By default, the window appears 30 seconds after the user navigates to the Workspace URL. You can set this value to 15, 30, 45 or 60 seconds. You can also disable the login timeout. If the login timeout is disabled, the window prompting users to work offline appears when the user navigates to the Workspace URL.

To configure the login timeout setting, click the extension icon in the browser on the user device. Use the window that appears to enable or disable login timeout and set the timeout duration:
An outage might prevent the user from logging in if the browser has been redirected to a third-party identity provider authentication site. In this case, the user can type the Workspace URL into the browser, which causes the window prompting users to work offline to appear. The user doesn’t have to wait through the login timeout interval for the window to appear.

Users can also access apps and desktops available during an outage this way:

1. Click the extension icon in the browser.
2. In the window that appears, click the button under **Work Offline**. This button says **Go to** and then the name of your Workspace store.
3. In the window that appears, click **Use Workspace Offline**.

During some outages, the warning window prompting users to work offline appears automatically when the extension detects Workspace-side issues. The user doesn’t need to take any action or wait through the login timeout interval.

**Browser limitations**

If users clear cookies and other site data in their browsers during an outage, service continuity doesn’t work until they authenticate to Workspace again.

Unless the user enables the extension to work in incognito mode, service continuity isn’t supported in incognito mode.
Troubleshooting for browser users

In the **Advanced** menu of the Citrix Workspace browser app account settings, ensure the current method for app and desktop launch preference is set to **Use Citrix Workspace App**. If this option is set to **Use Web Browser**, service continuity isn't supported in the browser.

Ensure that the extension icon in the browser appears green after the browser loads the Workspace URL.

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

---

**Fall back to StoreFront**

January 12, 2022

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

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

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

**Note:**

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

**Configure fall back to StoreFront**

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

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

**Download the PowerShell module**

Before you configure fall back to StoreFront, download and unpack the Citrix-provided PowerShell module from GitHub. The file includes Citrix.Workspace.FallbackConfiguration.psm1 and Citrix.Workspace.FallbackConfiguration.psd1

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

Citrix Cloud customers in the Japan region must also download the {json}production.json.{/json}

**Required configuration details**

To configure fall back to StoreFront, you need the following:

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

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

**Configure StoreFront fall back URLs**

1. Unzip the FallbackPowershellModule.zip file to a suitable directory from where you want to run the PowerShell, such as your current user’s desktop.

2. Open the PowerShell ISE and select **New** in the **File** menu.

3. Copy the example script into the interactive PowerShell window so that you can modify and run it against your own Citrix Cloud customer.

4. Set the $STFFallbackPath variable to the path of the directory that you unzipped the FallbackPowershellModule.zip file into.
5. Configure the $YourCustomerAPIKey, $YourCustomerSecretKey, and $YourCustomerURL variables in your PowerShell script with the information that you prepared in the Required configuration details step.

```powershell
$YourCustomerAPIKey = ""
$YourCustomerSecretKey = ""
$YourCustomerURL = "https://<yourcustomer>.cloud.com"
<!--NeedCopy-->
```

6. Import the PowerShell module

```powershell
if(Test-Path -Path "$STFFallbackPath\Citrix.Workspace.FallbackConfiguration.psm1") {
    Write-Host "Importing STF Fallback Powershell Module..." -ForegroundColor "Green"
    Import-Module -Name "$STFFallbackPath\Citrix.Workspace.FallbackConfiguration.psm1" -verbose
} else {
    Write-Host "STF Fallback Powershell Module not found inside $STFFallbackPath" -ForegroundColor "Red"
}
<!--NeedCopy-->
```

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

```powershell
Set-WorkspaceFallbackConfiguration -WorkspaceUrl $YourCustomerURL ` `-ClientId $YourCustomerAPIKey ` `-ClientSecret $YourCustomerSecretKey `
8. To verify that your StoreFront fall back URL has been configured correctly, follow the instructions under **View StoreFront fall back URLs**.

**View StoreFront fall back URLs**

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

```powershell
Get-WorkspaceFallbackConfiguration -WorkspaceUrl $YourCustomerURL `-ClientId $YourCustomerAPIKey `-ClientSecret $YourCustomerAPIKey `-Verbose
```

**Remove StoreFront fall back URLs**

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

```powershell
Remove-WorkspaceFallbackConfiguration -WorkspaceUrl $YourCustomerURL `-ClientId $YourCustomerAPIKey `-ClientSecret $YourCustomerSecretKey `-Verbose
```
Example script

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

```powershell

# Your credentials from Citrix Cloud Identity and Access Management
$string]$YourCustomerAPIKey = ""
[string]$YourCustomerSecretKey = ""

# Commercial US, EU or AP-S
[string]$YourCustomerURL = "https://<yourcustomer>.cloud.com"

# OR
# JP region
# [string]$YourCustomerURL = "https://<yourcustomer>.citrixcloud.jp"

# Unpack the .ZIP file containing the PowerShell module to a folder
# Point Import-Module to the same path where the Citrix.Workspace.
# FallbackConfiguration.psm1 file is
$STFFallbackPath = "$Env:UserProfile\Desktop\Fallback"

if(Test-Path -Path "$STFFallbackPath\Citrix.Workspace.
  FallbackConfiguration.psm1")
{
  Write-Host "Importing STF Fallback Powershell Module..." -
    ForegroundColor "Green"
  Import-Module -Name "$STFFallbackPath\Citrix.Workspace.
    FallbackConfiguration.psm1" -verbose
}
else
{
  Write-Host "STF Fallback Powershell Module not found inside
```
```powershell
$STFFallbackPath" -ForegroundColor "Red"
}

<# Uncomment lines 29 - 43 if your Citrix Cloud customer is in Japan #>

# Uses jp-production.json file to configure the $env:CTXWSPOSSETTINGS variable
$EnvironmentConfigFile = "jp-production.json"
if(Test-Path -Path "$STFFallbackPath\$EnvironmentConfigFile")
{
    Write-Host "Setting STF Fallback Environment Variables using $EnvironmentConfigFile..." -ForegroundColor "Green"
    $env:CTXWSPOSSETTINGS = "$STFFallbackPath\$EnvironmentConfigFile"
}

else
{
    Write-Host "Path to $EnvironmentConfigFile config file not found." -ForegroundColor "Red"
}

# Display detailed PowerShell help for the Fallback cmdlets
Get-Help Get-WorkspaceFallbackConfiguration -full
Get-Help Set-WorkspaceFallbackConfiguration -full
Get-Help Remove-WorkspaceFallbackConfiguration -full

# Perform Fallback admin tasks
# Get your existing configuration
Get-WorkspaceFallbackConfiguration -WorkspaceUrl $YourCustomerURL `-ClientId $YourCustomerAPIKey `-ClientSecret $YourCustomerAPIKey `-Verbose

# Add a new or overwrite/update the existing fallback config
Set-WorkspaceFallbackConfiguration -WorkspaceUrl $YourCustomerURL `-ClientId $YourCustomerAPIKey `-ClientSecret $YourCustomerSecretKey `-Configuration @{
```
Additional help and support

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

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

February 23, 2022

Citrix Federated Authentication Service (FAS) supports single sign-on (SSO) to virtual apps and desktops in Citrix Workspace. FAS is typically adopted if you're using one of the following identity providers for Citrix Workspace authentication:

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

With FAS, subscribers enter their credentials only once to access their virtual apps and desktops, just as they do with SaaS and Web apps.
FAS isn’t needed for SSO to virtual apps and desktops if you’re using Active Directory (AD), AD plus Token, or specific configurations of Citrix Gateway. For more information on configuring Citrix Gateway, visit Create an OAuth IdP policy on the on-premises Citrix Gateway.

**FAS servers**

Within each resource location, you can connect multiple FAS servers to Citrix Cloud for load balancing and failover purposes.

Citrix Cloud supports using FAS servers in the following scenarios.

In both scenarios, subscribers signing in to their workspaces through a federated identity provider enter their credentials only once to access apps and desktops.

**FAS servers connected with a single resource location**

If your resource locations contain varied infrastructure (for example, different resource locations contain different AD forests), deploy FAS servers to the resource location where your VDAs are. SSO is active only in resource locations where one or more FAS servers are connected.

**FAS servers connected with multiple resource locations**

If you have network connectivity between your resource locations and they contain similar infrastructure, you can connect your FAS servers with multiple resource locations. SSO is active for workspace subscribers who connect to virtual apps and desktops in those resource locations. In this scenario, there’s no need to connect separate FAS servers to each resource location.

When subscribers launch a virtual app or desktop, Citrix Cloud selects a FAS server in the same resource location as the app or desktop that is being launched. Citrix Cloud contacts the selected FAS server to obtain a ticket that grants access to a user certificate stored on the FAS server. To authenticate the subscriber, the VDA connects to the FAS server and presents the ticket.

You can use the same FAS server for both on-premises and Citrix Cloud with proper rule configuration.
Failover priority for multiple resource locations

When using FAS servers with multiple resource locations, FAS servers in one resource location can provide failover to FAS servers in other resource locations. When you add FAS servers to other resource locations, you designate each server as primary or secondary. When subscribers launch a virtual app or desktop, Citrix Cloud uses this designation in the following manner to select a FAS server:

- FAS servers that are designated as primary in the given resource location are considered first.
- If no primary servers are available, FAS servers that are designated as secondary are considered.
- If no secondary servers are available, the launch continues but single sign-on doesn’t occur.

Video overview

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

Requirements

Connectivity requirements

Use the FAS administration console to connect a FAS server to Citrix Cloud. You can use this console to configure a local or remote FAS server. To enable SSO for workspaces with FAS, the FAS administration console and FAS service access the following addresses using the console user’s account and Network Service account, respectively.

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

If your environment includes proxy servers, configure the user proxy with the addresses for the FAS administration console. Also, ensure that the address for the Network Service Account is configured as appropriate for your environment.
FAS system requirements

The requirements in this section apply to all FAS servers that you plan to connect with Citrix Cloud.

Complete system requirements for the FAS server are described in the System Requirements section of the FAS product documentation.

FAS servers in your on-premises Citrix Virtual Apps and Desktops environment must have Federated Authentication Service 2003 (Version 10.1) or later installed.

If your existing FAS server is older than Version 10, you can download the latest FAS software from Citrix and upgrade the server in-place before creating this connection. When you create the connection, you select the resource location for your FAS server. SSO is active for subscribers only in the resource locations where FAS servers are present.

For more information about upgrading an existing FAS server, see Install and configure in the FAS product documentation. The same FAS server can be used for Workspace and on-premises deployments.

Citrix Workspace

You must have the Citrix Virtual Apps and Desktops service provisioned and enabled in Workspace. By default, the Virtual Apps and Desktops service is enabled in Workspace Configuration after you subscribe to the service. However, the service requires that you deploy Citrix Cloud Connectors to allow Citrix Cloud to communicate with your on-premises environment.

Cloud Connectors

Citrix Cloud Connectors enable communication between your resource location (where the VDAs are) and Citrix Cloud. Deploy at least two Cloud Connectors to ensure high availability. The servers on which you install the Cloud Connector software must meet the following requirements:

- System requirements as described in Cloud Connector Technical Details
- No other Citrix components are installed, the server isn’t an Active Directory domain controller, and isn’t a machine critical to your resource location infrastructure.
- Joined to the domain where your VDAs are.

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

- Cloud Connector Proxy and Firewall Configuration
- Cloud Connector Installation

Setup overview

1. If you’re deploying new FAS servers, review the Requirements and follow the instructions in Install and configure FAS in this article.
2. Connect your FAS server to Citrix Cloud as described in Connect a FAS server to Citrix Cloud in this article. Completing this task connects your FAS server to a single resource location.

3. If you plan to connect your FAS server to multiple resource locations, follow the instructions in Add a FAS server to multiple resource locations in this article.

Install and configure FAS

Follow the FAS installation and configuration process described in the FAS product documentation. The configuration steps for StoreFront and the Delivery Controller aren’t required.

Tip:

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

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

Connect FAS servers to Citrix Cloud

Use the FAS administration console to connect your FAS server to Citrix Cloud as described in Install and configure in the FAS product documentation.

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

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

Add a FAS server to multiple resource locations

1. From the Citrix Cloud menu, select Resource Locations and then select the FAS Servers tab.
2. Locate the FAS server you want to manage, click the ellipsis (…) at the right side of the entry, and then select Manage Server.

3. Select Add to a resource location and then select the resource locations that you want.

4. Select Primary or Secondary for the FAS server’s failover priority in each selected resource location.

5. Select Save Changes.

To view the added FAS server, select Resource Locations from the Citrix Cloud menu and then select the FAS Servers tab. A list of all FAS servers for all connected resource locations appears. To display FAS servers for a specific resource location, select the resource location from the drop-down list.
Change a FAS server’s failover priority

1. From the Resource Locations page, select the FAS Servers tile for the resource location you want to manage.
2. Select the FAS Servers tab.
3. Locate the FAS server you want to manage, click the ellipsis at the right side of the entry, and then select Manage server.
4. Locate the resource location with the priority you want to change and select the new priority from the drop-down list.
5. Select Save Changes.

Enable federated authentication for workspaces

1. From the Citrix Cloud menu, select Workspace Configuration and then select Authentication.
2. Click Enable FAS. This change might take up to five minutes to be applied to subscriber sessions.
Afterward, the Federated Authentication Service is active for all virtual app and desktop launches from Citrix Workspace.
When subscribers sign in to their workspace and launch a virtual app or desktop in the same resource location as the FAS server, the app or desktop starts without prompting for credentials.

Note:

If all FAS servers in a resource location are down or in maintenance mode, application launches succeed, but single sign-on isn’t active. Subscribers are prompted for their AD credentials to access each application or desktop.

Remove a FAS server

To remove a FAS server from a single resource location:

1. From the Resource Locations page, select the FAS Servers tile for the resource location you want to manage.
2. Select the FAS Servers tab.
3. Locate the FAS server you want to manage, click the ellipsis at the right side of the entry, and
then select Manage server.

4. Locate the resource location you want to remove and then click the X icon.

To remove a FAS server from all connected resource locations:

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

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

If the FAS server isn’t available, a warning message appears on the FAS Servers page.

To diagnose the problem, open the FAS administration console on your on-premises FAS server and inspect the status. For example, the FAS server isn’t present in the FAS server GPO:
If the FAS administration console indicates that the server is operating properly, but there are still VDA logon problems, consult the FAS Troubleshooting Guide.

**Optimize workflows**

October 21, 2021

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

**Workspace Tools Starter Pack**

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

This starter pack is our guide for IT admins leveraging Citrix Workspace to improve employee experience and offers easy tools provided by Citrix to engage employees, monitor usage and feedback and measure the ROI of investing in a best class digital experience as you roll out Workspace to employees.
Integration options include Citrix Cloud admin status, Citrix Virtual Apps and Desktops service self-service apps, employee broadcast, FAQ and surveys to measure engagement, get feedback and understand employee satisfaction with Citrix Workspace.

Recommended apps and integrations:

- Citrix Cloud admin status
- Citrix Virtual Apps and Desktops service self-service
- Employee Broadcast
- Employee FAQ
- Employee Experience Survey

To find out more, see **Workspace Tools Starter Pack**.

**IT Self-service**

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

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

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

To find out more, see **IT Self-service**.
HR Self-service

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

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

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

To find out more, see HR Self-service.

Sales Productivity

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

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

To find out more, see Sales Productivity.

**Employee Well-being**

Deliver a workspace that integrates well-being into the way people like to work. There’s no doubt that employees can benefit from well-being tools that help them manage the stress and complexities of the workday. The challenge is getting those tools to employees without adding yet another item to their to-do list. Teams can use Citrix Workspace technology to improve the overall employee experience by delivering well-being tools and resources within an intelligent feed.
This use case is available through the Microapps service via our out-of-the-box template integrations with Citrix Podio. Available microapps include:

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

To find out more, see Employee Well-being.

**Video resources**

Check out these videos for demos of these workflows:

- IT Self-service microapp Demo
- HR Self-service microapp Demo
- Sales Productivity microapp Demo
- Employee Well-being Demo

**IT Self-service**

February 8, 2021

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

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

Citrix Workspace is unique in its ability to offer an indistinguishable experience to users regardless of location or device. It’s always the same, ensuring that employees remain productive and secure.

To help you get started, we have identified specific IT self-service workflows that results in improved employee productivity and employee satisfaction.

**Workflows**

This use case is available through the Microapps service via our out-of-the-box template integrations with ServiceNow, Zendesk, and JIRA and addresses these workflows:
Submit Incident – Quickly request help when you need it.

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

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

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

Integrations and microapps

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

ServiceNow

Set up the ServiceNow integration to get started. Manage subscribers for these microapps to enable the workflow:

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

Zendesk

Set up the Zendesk integration to get started. Manage subscribers for these microapps to enable the workflow:

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

Jira

Set up the Jira integration to get started. Manage subscribers for these microapps to enable the workflow:

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

Video resource

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

IT Self Service microapp Demo

HR Self-service

May 26, 2021

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

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

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

Workflows

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

Request PTO – Quickly submit time off requests.

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

© 1999–2022 Citrix Systems, Inc. All rights reserved.
Citrix Workspace

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

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

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

Integrations and microapps

This use case requires these integrations and the following microapps.

Workday

Set up the Workday integration to get started. Manage subscribers for these microapps to enable the workflow:

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

Set up the SAP SuccessFactors integration to get started. Manage subscribers for these microapps to enable the workflow:

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

Kronos Workforce Central

Set up the Kronos Workforce Central integration to get started. Manage subscribers for these microapps to enable the workflow:

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

Video resource

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

HR Self Service microapp Demo

Sales Productivity

March 23, 2021

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

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

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

Workflow

This use case is available through the Microapps service via our out-of-the-box template integrations with Salesforce and MS Dynamics CRM, and addresses these workflows:
Opportunity Updates – Quickly edit opportunity and view opportunity details.

Task Management – Improve productivity with real-time notifications.

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

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

Search – Personalized search experience for sales related admin tasks.

Integrations and microapps

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

SalesForce

Set up the SalesForce integration to get started. Manage subscribers for these microapps to enable the workflow:

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

MS Dynamics CRM

Set up the MS Dynamics CRM to get started. Manage subscribers for these microapps to enable the workflow:
Citrix Workspace

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

**Video Resource**

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

*Sales Productivity microapp Demo*

**Employee Well-being**

February 9, 2021

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

**Workflow**

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

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

**Good News** – Increase employee morale by sharing positivity across your organization with our Broadcast microapps.
Citrix Podio integration template and microapps

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

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

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

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

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

Check out the Employee Well-Being App Pack for more inspirational ideas.

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

Video resource

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

Employee Well-being Demo