Citrix DaaS for Azure

Contents

Citrix DaaS Standard for Azure

August 30, 2022

Introduction

Citrix DaaS Standard for Azure (formerly Citrix Virtual Apps and Desktops Standard for Azure) is the simplest, fastest way to deliver Windows apps and desktops from Microsoft Azure. Citrix DaaS for Azure offers cloud-based management, provisioning, and managed capacity for delivering virtual apps and desktops to any device.

This solution includes:

- Cloud-based management and provisioning for delivering Citrix-hosted Azure Virtual Desktops, and apps from multi-session machines.
- A high-definition user experience from a broad range of devices, using the Citrix Workspace app.
- Simplified image creation and management workflows, along with Citrix prepared Windows and Linux single-session and multi-session images that have the latest Citrix Virtual Delivery Agent (VDA) installed.
- Secure remote access from any device using global points of presence of the Citrix Gateway service.
- Advanced monitoring and help desk management capabilities.
- Managed Azure IaaS, including Azure compute, storage, and networking for delivering virtual desktops.

The Citrix Remote PC Access feature enables users to remotely use existing physical machines located in the office. Users receive the best user experience by using Citrix HDX to deliver their office PC session.

If you're familiar with other Citrix DaaS products, Citrix DaaS for Azure simplifies the deployment of virtual apps and desktops. Citrix can manage the infrastructure for hosting those workloads.

Citrix DaaS for Azure is a Citrix Cloud service. Citrix Cloud is the platform that hosts and administers Citrix Cloud services. Learn more about Citrix Cloud.

To learn about components, data flow, and security considerations, see Technical security overview. That article also outlines customer and Citrix responsibilities.

How users access desktops and apps

Users (sometimes called subscribers) access their desktops and apps directly through their browser, using the Citrix HTML5 client. Users browse to a Citrix Workspace URL that is provided by you, their

administrator. The Citrix Workspace platform enumerates and delivers the digital resources to users. Users start a desktop or an application from their workspace.

After you configure a catalog of machines that deliver desktops and apps (or a catalog containing physical machines for Remote PC Access), Citrix DaaS for Azure displays the Workspace URL. You then notify your users to go to that URL to start their desktop and apps.

As an alternative to navigating to Citrix Workspace to access their desktops and apps, users can install a Citrix Workspace app on their device. Download the app that's right for the endpoint device's operating system: https://www.citrix.com/downloads/workspace-app/.

Concepts and terminology

This section introduces some of the items and terms that administrators use in Citrix DaaS for Azure:

- Catalogs
- Resource locations
- Images
- Azure subscriptions
- Network connections
- Domain-joined and non-domain-joined

Catalogs

A catalog is a group of machines.

- The desktops and apps that Citrix DaaS for Azure delivers to your users reside on virtual machines (VMs). Those VMs are created (provisioned) in the catalog.

  When you deploy desktops, the machines in the catalog are shared with selected users. When you publish applications, multi-session machines host applications that are shared with selected users.

- For Remote PC Access, a catalog contains existing single-session physical machines. A common deployment includes machines located in your office. You control user access to those machines through the configured user assignment method and selected users.

If you're familiar with other Citrix DaaS products, a catalog in Citrix DaaS is similar to combining a machine catalog and a delivery group.

For more information, see:

- Create catalogs for published desktops and apps.
- Create catalogs for Remote PC Access.

- Manage catalogs.
- Users and authentication.

Resource locations

A catalog's machines reside in a resource location. A resource location also contains two or more Cloud Connectors.

- When publishing desktops or apps, Citrix automatically creates the resource location and the Cloud Connectors when you create the first catalog.
- For Remote PC Access, the administrator creates the resource location and the Cloud Connectors before creating a catalog.

When you create more catalogs for published desktops and apps, the Azure subscription, region, and domain determine whether Citrix creates another resource location. If those criteria match an existing catalog, Citrix tries to reuse that resource location.

For more information, see:

- Specify resource location information when you create a catalog.
- Resource location actions.

Images

When you create a catalog for published desktops and apps, a machine image is used (with other settings) as a template for creating the machines.

- Citrix DaaS for Azure provides several Citrix prepared images:
  - Windows 10 Enterprise (single-session)
  - Windows 10 Enterprise Virtual Desktop (multi-session)
  - Windows 10 Enterprise Virtual Desktop (multi-session) with Office 365 ProPlus
  - Windows Server 2012 R2
  - Windows Server 2016
  - Windows Server 2019
  - Linux

  Each Citrix prepared image has a Citrix VDA and troubleshooting tools installed. The VDA is the communication mechanism between your users' machines and the Citrix Cloud infrastructure that manages Citrix DaaS for Azure.

  Citrix updates the available prepared images when a new VDA version releases.

- You can also import and use your own images from Azure. You must install a VDA (and other software) on the image before it can be used to create a catalog.

The term VDA often refers to the machine that delivers apps or desktops, and the software component installed on that machine.

For more information, see Images.

Azure subscriptions

You can create catalogs for delivering desktops and apps, and build/import images in either in a Citrix Managed Azure subscription or your own (customer-managed) Azure subscription.

If you order only Citrix DaaS for Azure, you must import (add) and use your own Azure subscriptions. If you also order a Citrix Azure Consumption Fund, you receive a Citrix Managed Azure subscription. You can then use either a Citrix Managed Azure subscription or one of your imported Azure subscriptions when creating a catalog or building a new image.

For more information, see:

- Deployment scenarios illustrate ways to use Azure subscriptions with Citrix DaaS for Azure.
- Azure subscriptions explains the differences between Citrix Managed Azure and customer-managed Azure subscriptions. This article also describes how to view, add, and remove subscriptions.
- Technical security overview describes the differences in responsibility with Citrix Managed Azure and customer-managed Azure subscriptions.

Network connections

When creating a catalog using a Citrix Managed Azure subscription, you indicate if and how users can access locations and resources on their corporate on-premises network from their published desktops and apps. The choices are no connectivity, Azure VNet peering, and Citrix SD-WAN.

When using your own Azure subscription, there is no need to create a connection. You only need to import (add) your Azure subscription to the service.

For more information, see Network connections.

Domain-joined and non-domain-joined

Several service operations and features differ, depending on whether the machines (VDAs) are domain-joined or non-domain-joined. Domain membership also affects the available deployment scenarios.

- Both domain-joined and non-domain joined machines support any of the user authentication methods available in the user's workspace.
- You can publish desktops, apps, or both from domain-joined and non-domain-joined machines. Machines in Remote PC Access catalogs must be domain-joined.

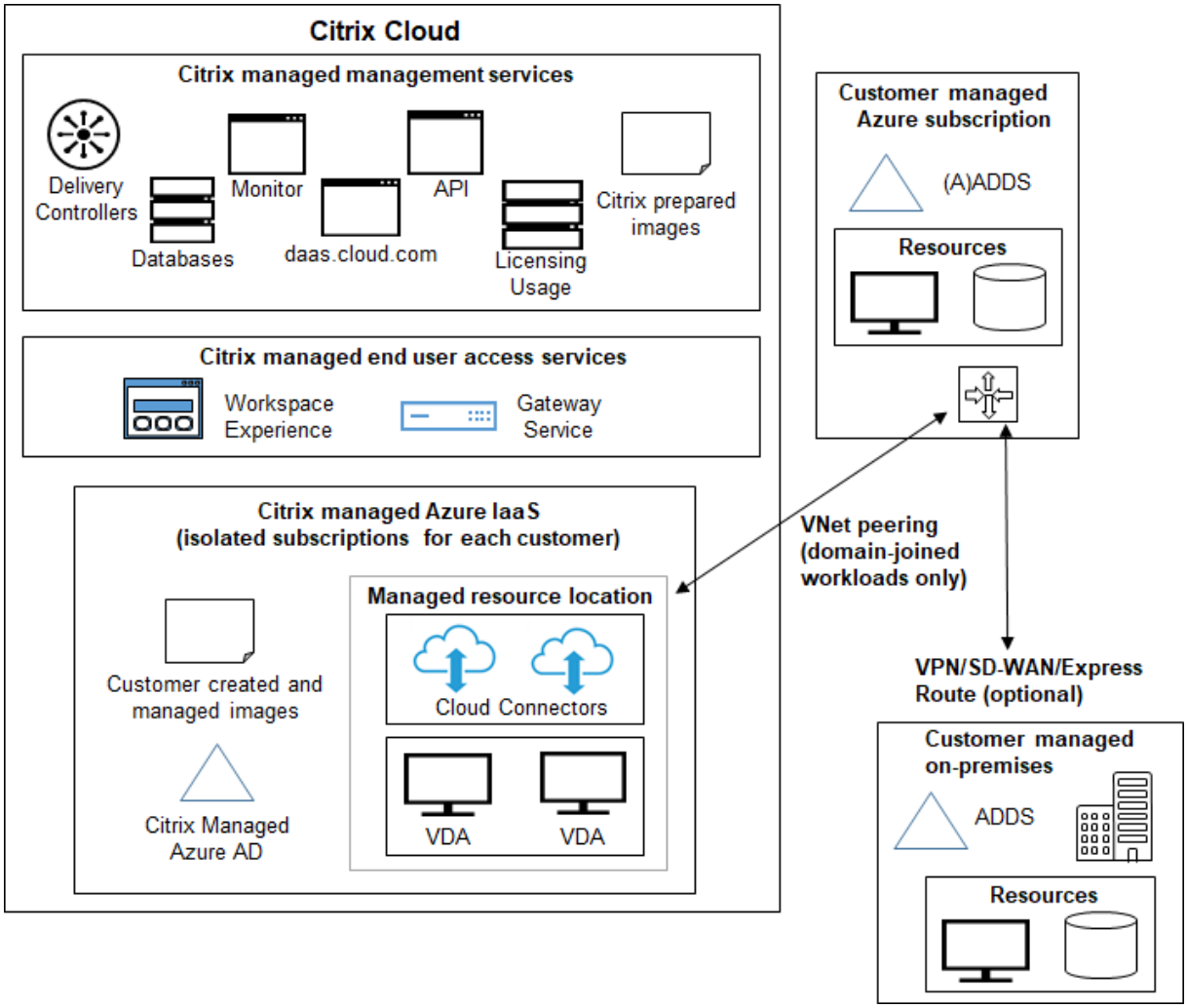
The following table lists several differences between non-domain-joined and domain-joined machines when delivering desktops and apps.

Non-domain-joined	Domain-joined
Active Directory is not used for machines. Machines are not joined to an AD domain.	Active Directory is used for machines. Machines are joined to an AD domain.
Active Directory group policies cannot be applied to machines (VDAs). (You can apply local GPO on the image that's used to create a catalog.)	VDAs inherit group policies for the AD OU specified during catalog creation.
Users sign in using single sign-on.	When users sign in to their workspace using an authentication method other than Active Directory, they are also prompted for sign-in when a desktop or app launches.
Do not need a connection to an on-premises network.	(When using a Citrix Managed Azure subscription) Must have a connection to access an on-premises network, using Microsoft Azure VNet or Citrix SD-WAN.
Must use a Citrix Managed Azure subscription for provisioning VDAs. (Cannot use your own Azure subscriptions for provisioning VDAs. However, users can be connected from your own Azure AD.)	Can use a Citrix Managed Azure subscription and your own Azure subscriptions.
Cannot troubleshoot using a bastion machine or direct RDP.	Can troubleshoot using a bastion machine or direct RDP.
Cannot use Citrix Profile Management. (Recommend: Use persistent catalogs.)	Can use Citrix Profile Management or FSLogix.

Deployment scenarios

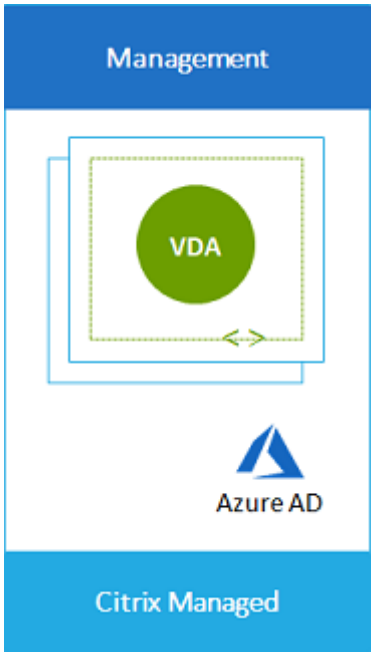
Deployment scenarios for published desktops and apps differ, depending on whether you're using a Citrix Managed Azure subscription or your own customer-managed Azure subscription.

Deploying in a Citrix Managed Azure subscription

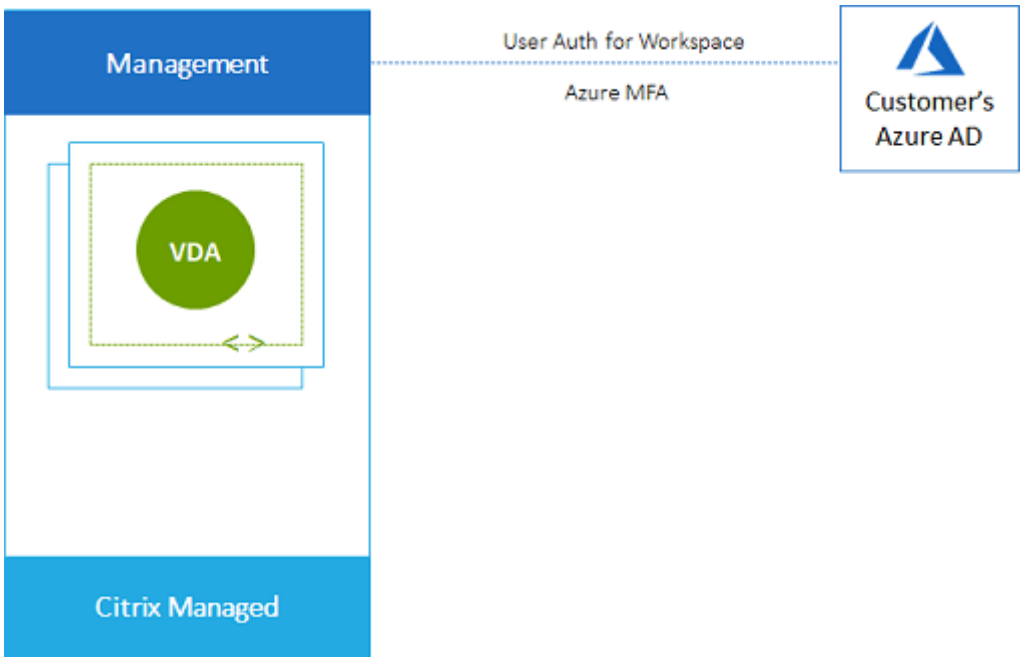


Citrix DaaS for Azure supports several deployment scenarios for connection and user authentication.

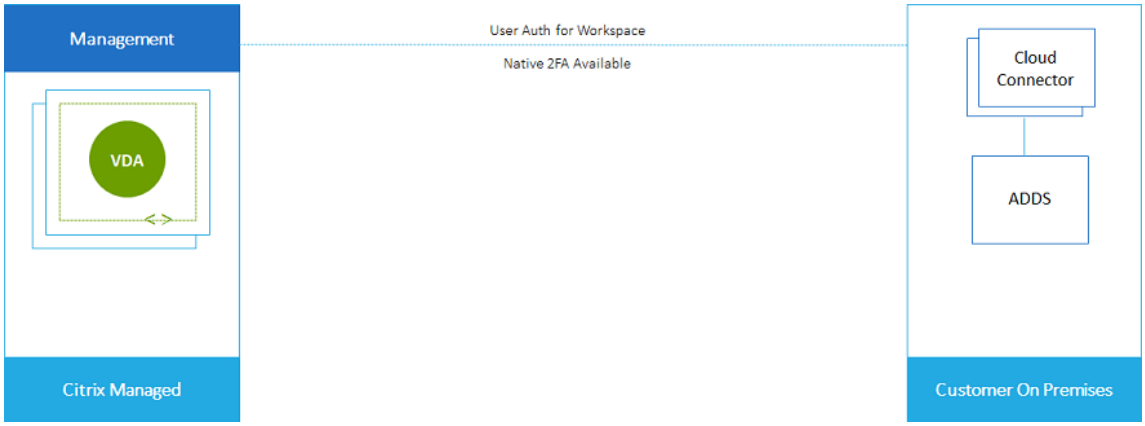
- **Managed Azure AD:** This is the simplest deployment, with non-domain-joined VDAs. It's recommended for proofs of concept. You use the Managed Azure AD (which Citrix manages) to manage users. Your users don't need to access resources on your on-premises network.



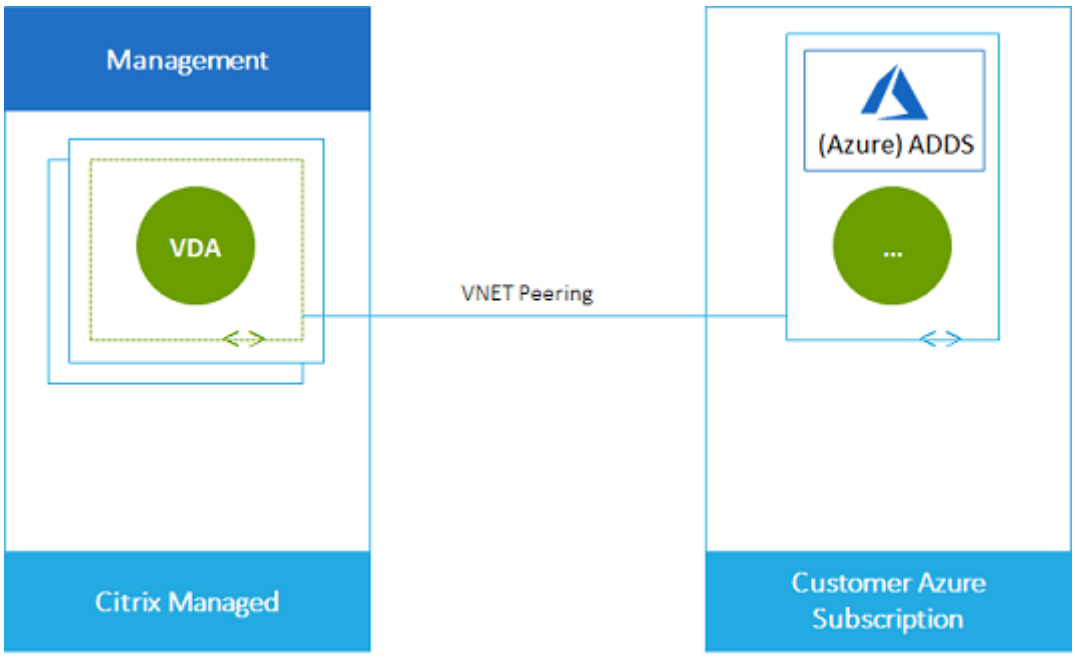
- **Customer's Azure Active Directory:** This deployment contains non-domain-joined VDAs. You use your own Active Directory or Azure Active Directory (AAD) for end user authentication. In this scenario, your users don't need to access resources on your on-premises network.



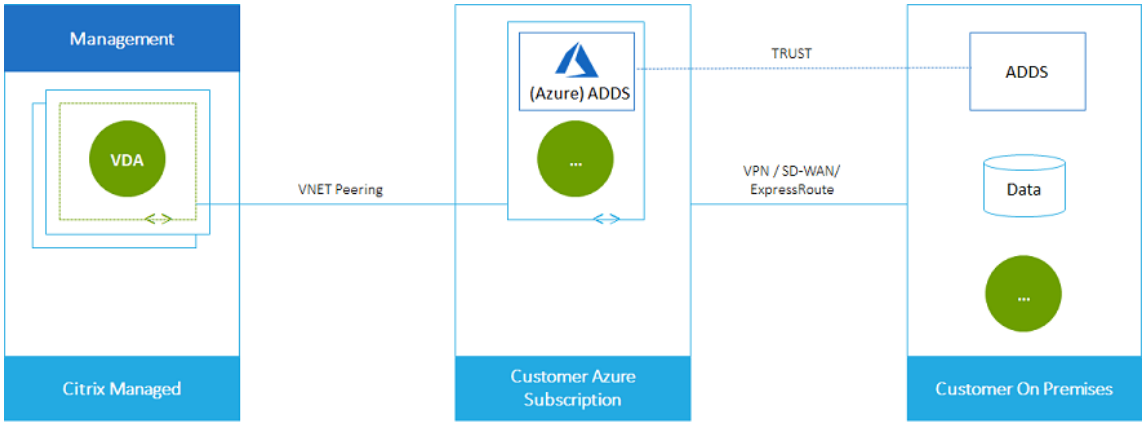
- **Customer's Azure Active Directory with on-premises access:** This deployment contains non-domain-joined VDAs. You use your own AD or AAD for end user authentication. In this scenario, installing Citrix Cloud Connectors in your on-premises network enables access to resources in that network.



- **Customer's Azure Active Directory Domain Services and VNet peering:** If your AD or AAD resides in your own Azure VNet and Azure subscription, you can use the Microsoft Azure VNet peering feature for a network connection, and Azure Active Directory Domain Services (AADDS) for end user authentication. The VDAs are joined to your domain.

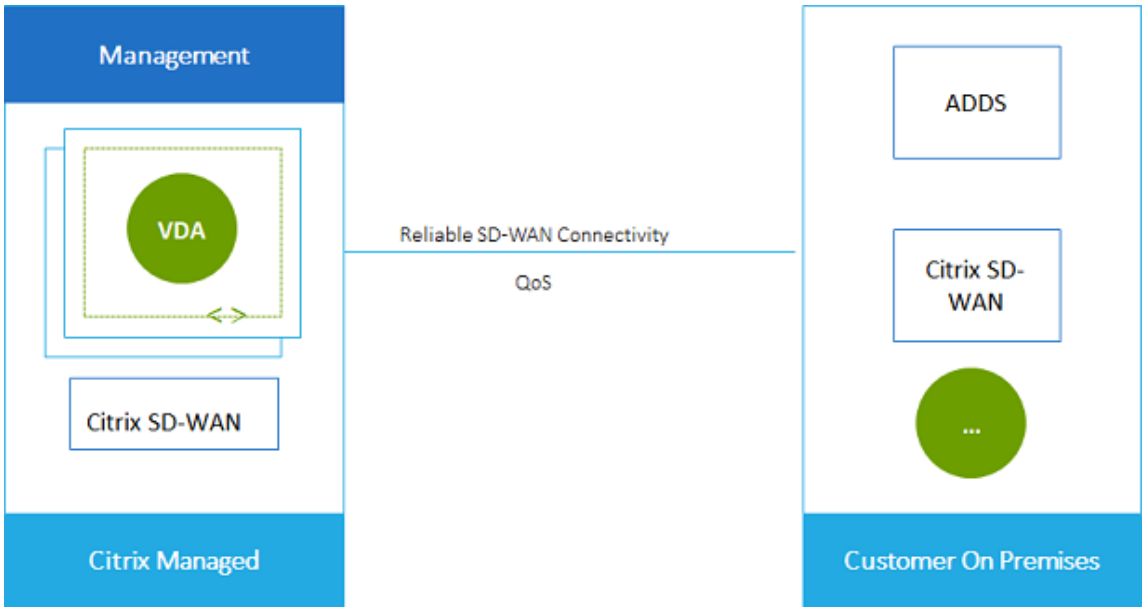


To enable your users to access data stored in your on-premises network, you can use your VPN connection from your Azure subscription to the on-premises location. Azure VNet peering is used for network connectivity. Active Directory Domain Services in the on-premises location is used for end user authentication.

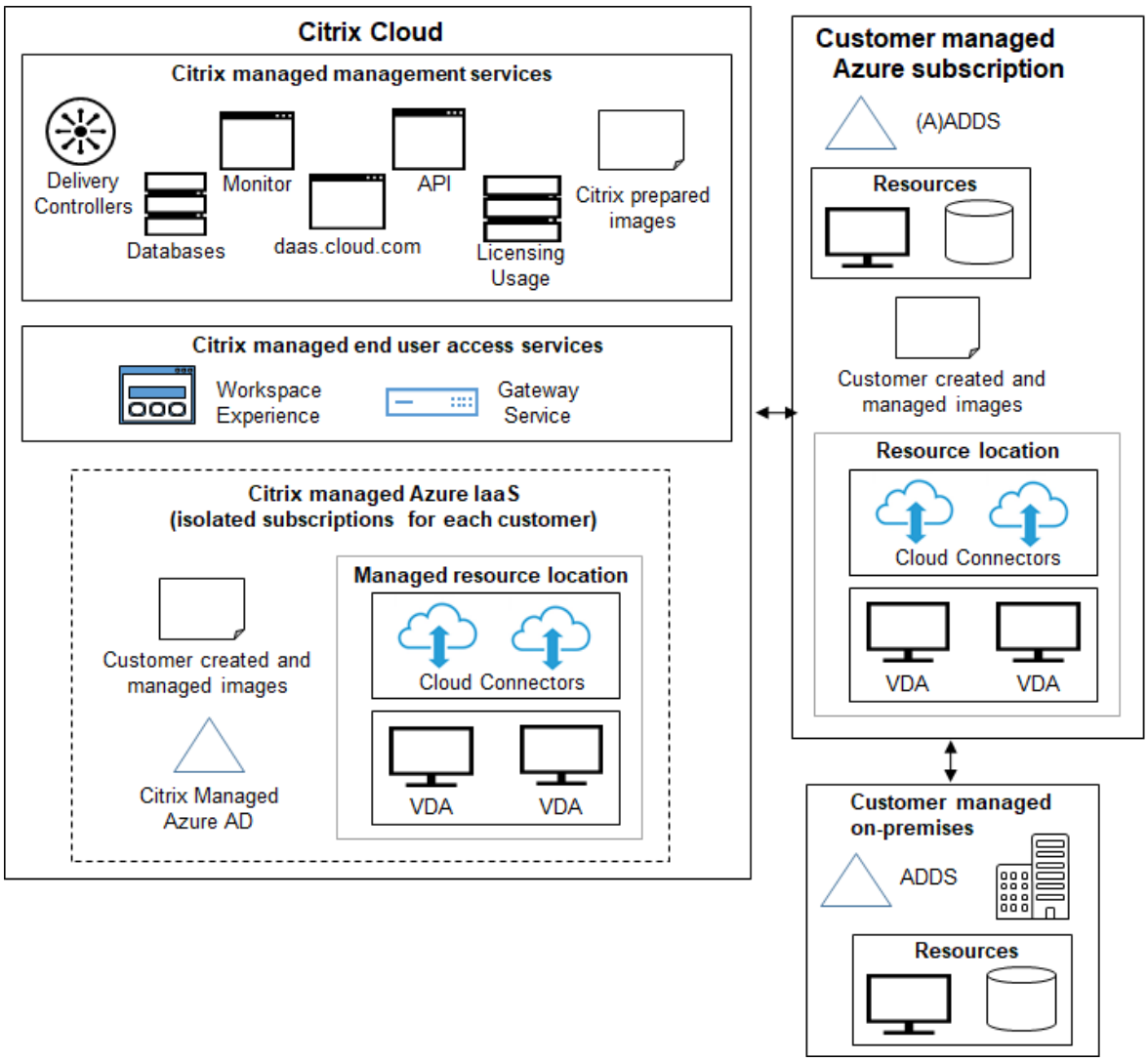


- **Customer's Active Directory and SD-WAN:** You can provide users with access to files and other items from your on-premises or cloud SD-WAN networks.

  Citrix SD-WAN optimizes all the network connections needed by Citrix DaaS for Azure. Working in concert with the HDX technologies, Citrix SD-WAN provides quality-of-service and connection reliability for ICA and out-of-band Citrix DaaS for Azure traffic.



Deploying in a customer managed Azure subscription



The deployment in the preceding graphic uses a customer-managed Azure subscription. However, the Citrix Managed Azure subscription remains an option for other catalogs and images, as indicated by the dotted outline.

Management interfaces

Citrix DaaS for Azure has two graphical management interfaces: Quick Deploy and Full Configuration.

- **Quick Deploy** enables you to quickly create catalogs and start delivering desktops and apps to your users. (Hence the name, Quick Deploy.) It's the default interface when you start Citrix DaaS for Azure. You can also access this interface by selecting **Manage > Azure Quick Deploy**. The instructions in this product documentation set assume you're using Quick Deploy.

If you plan to use a Citrix Managed Azure subscription when creating a catalog or image, you must use Quick Deploy.

- **Full Configuration** offers advanced features and configuration options to tailor and manage your deployment. Catalogs that you create in Quick Deploy automatically appear in Full Configuration. To move from Quick Deploy to Full Configuration, select **Manage > Full Configuration**.

  When you create a catalog in Quick Deploy, an associated delivery group and host connection are created automatically in Full Configuration.

  Full Configuration also offers its own catalog creation process that includes creating a connection to the Azure host, then creating a catalog and a delivery group. That process is supported only if you use your own Azure subscription. It's much easier to create the catalog in Quick Deploy.

  Full Configuration supports processes related to hypervisor and cloud service hosts other than Azure. Those are not available to Citrix DaaS for Azure customers.

Manage catalogs created in the Quick Deploy interface

After you create a catalog in the Quick Deploy interface, you can continue to manage that catalog in that interface. For details, see Manage catalogs. You can also use the Full Configuration interface.

When you create a catalog in Quick Deploy, that catalog (plus the delivery group and hosting connection that are created automatically behind the scenes) are assigned a scope of `Citrix managed object`. Scopes are used in delegated administration to group objects.

Catalogs, delivery groups, and connections with the `Citrix managed object` scope are prohibited from certain actions in the Full Configuration interface. (Allowing those actions in Full Configuration might adversely affect the system's ability to support both Quick Deploy and Full Configuration, so those actions are disabled.) In the Full Configuration interface:

- **Catalog:** Most of the catalog management actions are not available. You cannot delete a catalog.
- **Delivery group:** Most of the delivery group management actions are available. You cannot delete the delivery group.
- **Connection:** Most of the connection management actions are not available. You cannot delete a connection. You cannot create a connection that is based on a connection that has the `Citrix managed object` scope.

If you create a catalog in Quick Deploy using your own Azure subscription (that you added to Quick Deploy), and you want to manage the catalog (and its delivery group and connection) entirely in Full Configuration, you can *convert* the catalog.

- Converting a catalog restricts its management to only the Full Configuration interface. After a catalog is converted, you can no longer use the Quick Deploy interface to manage that catalog.
- After a catalog is converted, the actions that were previously unavailable in Full Configuration can be selected. (The `Citrix managed object` scope is removed from the converted catalog, delivery group, and hosting connection.)
- To convert a catalog:

  From the **Manage > Azure Quick Deploy** dashboard in Citrix DaaS for Azure, click anywhere in the catalog's entry. On the **Details** tab, under **Advanced settings**, select **Convert Catalog**. When prompted, confirm the conversion.
- You cannot convert a catalog that was created in Quick Deploy using a Citrix Managed Azure subscription.

For information about how to manage converted catalogs in Full Configuration, see:

- Manage machine catalogs (Full Configuration refers to catalogs as machine catalogs)
- Manage delivery groups

More information

For technical details, see:

- Citrix Tech Zone reference architecture
- Citrix Tech Zone tech brief

For information about automating your deployments, see the Managed desktops public API preview.

When you're ready, get started.

What's new

August 9, 2023

A goal of Citrix is to deliver new features and product updates to Citrix DaaS for Azure customers when they are available. New releases provide more value, so there's no reason to delay updates. To you, the customer administrator, this process is transparent.

Citrix prepared image updates

The Citrix prepared images have a current Citrix Virtual Delivery Agent (VDA) installed. Generally, new VDA versions are released several times each year, and the available Citrix prepared images are automatically updated with the latest VDA. To learn about new and enhanced features in the VDA's current version, see:

- Windows VDAs
- Linux VDAs

August 2022

- This feature is generally available: You can now create catalogs of machines joined to your Azure Active Directory. See Create catalogs.

May 2022

- You can now create catalogs of machines joined to your Azure Active Directory. This feature is in preview. See Create catalogs.
- Citrix Service Providers can now remove the Citrix DaaS for Azure service from customers. See Remove a Service.

April 2022

- Host connection creation for Citrix Hypervisor, Microsoft SCVMM, VMware vSphere, Prism Central, and Nutanix AHV is now available. As such, you can now use on-premises hypervisors in addition to Azure.
- Product name change from Citrix Virtual Apps and Desktops Standard for Azure to Citrix DaaS Standard for Azure. For more information about the rebranding of all Citrix DaaS (formerly Citrix Virtual Apps and Desktops service) offerings, see What's New in Citrix DaaS. Learn more about the name changes at our announcement on our blog.

January 2022

- When you create catalogs, you can now store your machines on standard SSD storage. Previously, only standard disks (HDD) and premium SSD were supported.
- Support for these new regions for hosting VDA workloads: Brazil South, Central India, Japan East, South Central US, and UK South.

- Snapshots and restore are now available for persistent desktops hosted on Citrix Managed Azure and BYO Azure. See VDA snapshot and restore.
- Static public IP address for all outbound traffic from VDAs hosted are now available. You can configure an Azure NAT Gateway to get the IP address. See Create a public static IP address.
- Azure VPN is available for technical preview. Azure VPN lets you connect Citrix Managed Azure directly with on-premises data centers. See Azure VPN Technical Preview.
- New Linux images are available for Citrix prepared images.

November 2021

- Auto-approved 7-day trials are now available (in addition to sales-approved trials).
- Citrix Service Providers can now manage users from the service's **Manage > Azure Quick Deploy** dashboard or the Citrix Cloud console. For details, see Partner access to customer identity provider.

October 2021

- New information about managing catalogs created in Quick Deploy.

September 2021

- Preview API content is available.
- Support for Windows Server 2022 (requires minimum VDA 2106).

July 2021

- Web Studio management interface renamed Full Configuration.

June 2021

- Support for two management interfaces: Quick Deploy and Web Studio.

May 2021

- This service supports the Service Continuity preview.
- Citrix prepared images now include Ubuntu single-sesssion and multi-session versions.

- When adding a Cloud Connector to a resource location, using a Citrix Managed Azure subscription, you can specify the Cloud Connector machine's performance type.
- When creating a catalog, the machine performance choices include options that match the generation type (gen1 or gen2) of the image you selected. You can update a catalog with a different generation type image, if the catalog's machines support that generation type.

April 2022

- Product name change from Citrix Virtual Apps and Desktops Standard for Azure to Citrix DaaS Standard for Azure.

January 2021

- Preview support for viewing consumption commitment usage.

October 2020

- You can use the Monitor shadow feature to view or work on a user's VM or session.
- Production support for Remote PC Access.
- Enhanced catalog creation option to use your Azure Virtual Desktop eligible license or Azure Hybrid Benefit.
- If a restart action on a machine is unsuccessful, you can use a force restart action.

September 2020

- Details about images are reorganized and expanded. For example, you can now add and edit notes about images that you prepared or imported. You can also limit access to only specified IP addresses.
- When creating an Azure VNet peering connection that will use an Azure virtual network gateway, you can now also enable virtual network gateway route propagation.
- Product name change from Citrix Managed Desktops to Citrix Virtual Apps and Desktops Standard for Azure.

August 2020

- Preview support for Remote PC Access.
- A Citrix prepared Windows Server 2019 image is now available.

July 2020

- When adding a Cloud Connector to a resource location, using a customer-managed Azure subscription, you can specify the Cloud Connector machine's performance type and Azure resource group. For details, see Resource location actions.
- When creating a catalog, you can specify a machine naming scheme. See Create a catalog using custom create.

June 2020

- In a CSP environment, SD-WAN connections are created on a per-tenant basis. For the SD-WAN connection option to be available to the CSP administrator, the tenant must have an SD-WAN Orchestrator service entitlement. For details, see Filter resources by customer (multitenant deployments).
- Production support for Linux VDAs when using a customer-managed Azure subscription.
- The limit of VDAs per subscription is now 1,200.

May 2020

- You can add another Citrix Managed Azure subscription when you need more machines than the limit per Citrix Managed Azure subscription.
- Additional information about DNS servers.

March 2020

- Production support for SD-WAN connections.

February 2020

- To view your Citrix license usage information, follow the guidance in Monitor license and usage monitoring for Citrix DaaS Standard for Azure.
- Preview support for catalogs containing Red Hat Enterprise Linux or Ubuntu machines. This feature is valid only when using a customer-managed Azure subscription, and requires an imported image containing a Citrix Linux VDA.
- You can now configure either vertical or horizontal load balancing for all of your multi-session machines. (Previously, all machines used horizontal load balancing.) This global selection applies to all catalogs in your deployment. See Load balancing.
- You can now add an Azure subscription if you're not a Global Admin.

- A Citrix prepared image is now available for Windows 10 Enterprise Virtual Desktop (multi-session) with Office 365 ProPlus.

January 2020

- Add support for custom routes in VNet peering connections.
- Updates to security article to enhance port and rules information.

November 2019

- Preview support for SD-WAN connections.

October 2019

- In Supported operating systems, added entries for:
  - Windows 7 (supports only VDA 7.15 with the latest Cumulative Update).
  - Windows Server 2019.
- A Windows Server 2012 R2 Citrix prepared image is now available.
- Added resource location settings information. For details, see Resource location actions and Resource location settings when creating a catalog.

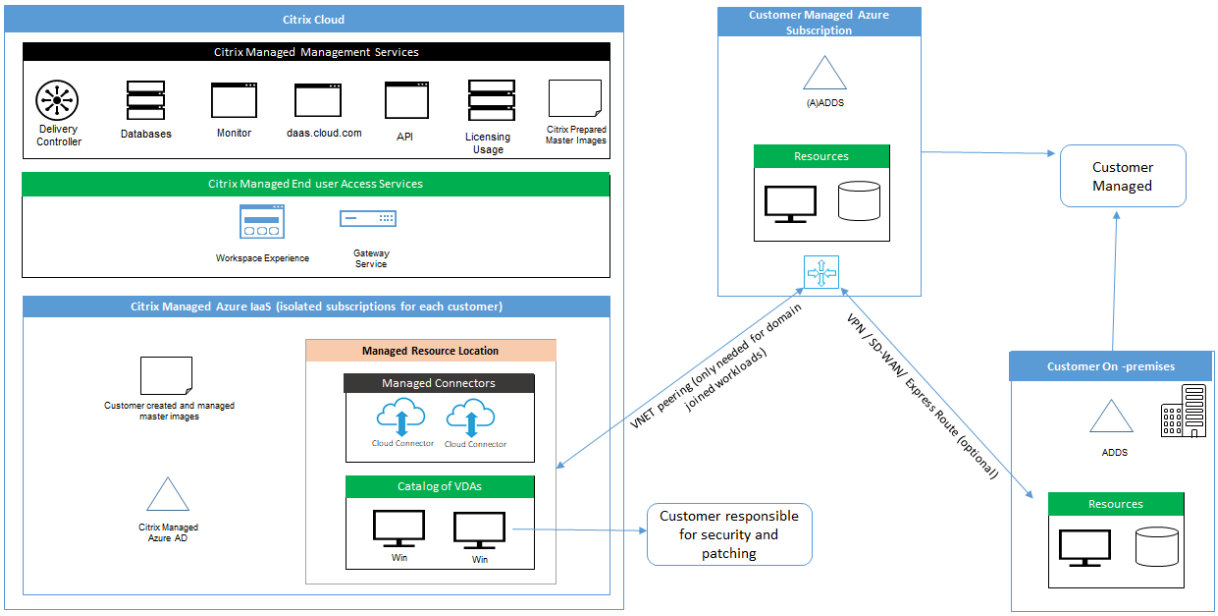
September 2019

- By default, machines are created in a Citrix Managed Azure subscription. Now you can also create catalogs and images in your own customer-managed Azure subscription.

Technical security overview

April 21, 2022

The following diagram shows the components in a Citrix DaaS Standard for Azure (formerly Citrix Virtual Apps and Desktops Standard for Azure) deployment. This example uses a VNet peering connection.



With Citrix DaaS for Azure, the customer's Virtual Delivery Agents (VDAs) that deliver desktops and apps, plus Citrix Cloud Connectors, are deployed into an Azure subscription and tenant that Citrix manages.

> **NOTE:**
>
> This article provides an overview of security requirements for customers deploying Citrix DaaS for Azure using a Citrix Managed Azure subscription. For an architectural overview of a deployment of Citrix DaaS for Azure using a customer-managed Azure subscription, including security information, see Reference Architecture: Virtual Apps and Desktops Service - Azure.

Citrix cloud-based compliance

As of January 2021, the use of Citrix Managed Azure Capacity with various Citrix DaaS editions and Workspace Premium Plus has not been evaluated for Citrix SOC 2 (Type 1 or 2), ISO 27001, HIPAA, or other cloud compliance requirements. Visit the Citrix Trust Center for more information regarding Citrix Cloud Certifications, and check back frequently for updates.

Citrix responsibility

Citrix Cloud Connectors for non-domain-joined catalogs

Citrix DaaS for Azure deploys at least two Cloud Connectors in each resource location. Some catalogs may share a resource location if they are in the same region as other catalogs for the same customer.

Citrix is responsible for the following security operations on non-domain-joined catalog Cloud Connectors:

- Applying operating system updates and security patches
- Installing and maintaining antivirus software
- Applying Cloud Connector software updates

Customers do not have access to the Cloud Connectors. Therefore, Citrix is wholly responsible for the performance of the non-domain-joined catalog Cloud Connectors.

Azure subscription and Azure Active Directory

Citrix is responsible for the security of the Azure subscription and Azure Active Directory (AAD) that are created for the customer. Citrix ensures tenant isolation, so each customer has their own Azure subscription and AAD, and cross-talk between different tenants is prevented. Citrix also restricts access to the AAD to the Citrix DaaS for Azure and Citrix operations personnel only. Access by Citrix to each customer's Azure subscription is audited.

Customers employing non-domain-joined catalogs can use the Citrix-managed AAD as a means of authentication for Citrix Workspace. For these customers, Citrix creates limited privilege user accounts in the Citrix-managed AAD. However, neither customers'users nor administrators can execute any actions on the Citrix-managed AAD. If these customers elect to use their own AAD instead, they are wholly responsible for its security.

Virtual networks and infrastructure

Within the customer's Citrix Managed Azure subscription, Citrix creates virtual networks for isolating resource locations. Within those networks, Citrix creates virtual machines for the VDAs, Cloud Connectors, and image builder machines, in addition to storage accounts, Key Vaults, and other Azure resources. Citrix, in partnership with Microsoft, is responsible for the security of the virtual networks, including virtual network firewalls.

Citrix ensures the default Azure firewall policy (network security groups) is configured to limit access to network interfaces in VNet peering and SD-WAN connections. Generally, this controls incoming traffic to VDAs and Cloud Connectors. For details, see:

- Firewall policy for Azure VNet peering connections
- Firewall policy for SD-WAN connections

Customers cannot change this default firewall policy, but may deploy additional firewall rules on Citrix-created VDA machines; for example, to partially restrict outgoing traffic. Customers that install virtual private network clients, or other software capable of bypassing firewall rules, on Citrix-created VDA machines are responsible for any security risks that might result.

When using the image builder in Citrix DaaS for Azure to create and customize a new machine image, ports 3389-3390 are opened temporarily in the Citrix-managed VNet, so that the customer can RDP to the machine containing the new machine image, to customize it.

Citrix responsibility when using Azure VNet peering connections

For VDAs in Citrix DaaS for Azure to contact on-premises domain controllers, file shares, or other intranet resources, Citrix DaaS for Azure provides a VNet peering workflow as a connectivity option. The customer's Citrix-managed virtual network is peered with a customer-managed Azure virtual network. The customer-managed virtual network may enable connectivity with the customer's on-premises resources using the cloud-to-on-premises connectivity solution of the customer's choice, such as Azure ExpressRoute or iPsec tunnels.

Citrix responsibility for VNet peering is limited to supporting the workflow and related Azure resource configuration for establishing peering relationship between Citrix and customer-managed VNets.

Firewall policy for Azure VNet peering connections Citrix opens or closes the following ports for inbound and outbound traffic that uses a VNet peering connection.

Citrix-managed VNet with non-domain-joined machines

- Inbound rules
  - Allow ports 80, 443, 1494, and 2598 inbound from VDAs to Cloud Connectors, and from Cloud Connectors to VDAs.
  - Allow ports 49152-65535 inbound to the VDAs from an IP range used by the Monitor shadowing feature. See Communications Ports Used by Citrix Technologies.
  - Deny all other inbound. This includes intra-VNet traffic from VDA to VDA, and VDA to Cloud Connector.
- Outbound rules
  - Allow all traffic outbound.

Citrix-managed VNet with domain-joined machines

- Inbound rules:
  - Allow ports 80, 443, 1494, and 2598 inbound from the VDAs to Cloud Connectors, and from Cloud Connectors to VDAs.
  - Allow ports 49152-65535 inbound to the VDAs from an IP range used by the Monitor shadowing feature. See Communications Ports Used by Citrix Technologies.

  - Deny all other inbound. This includes intra-VNet traffic from VDA to VDA, and VDA to Cloud Connector.

- Outbound rules
  - Allow all traffic outbound.

Customer-managed VNet with domain-joined machines

- It is up to the customer to configure their VNet correctly. This includes opening the following ports for domain joining.
- Inbound rules:
  - Allow inbound on 443, 1494, 2598 from their client IPs for internal launches.
  - Allow inbound on 53, 88, 123, 135-139, 389, 445, 636 from Citrix VNet (IP range specified by customer).
  - Allow inbound on ports opened with a proxy configuration.
  - Other rules created by customer.
- Outbound rules:
  - Allow outbound on 443, 1494, 2598 to the Citrix VNet (IP range specified by customer) for internal launches.
  - Other rules created by customer.

Citrix responsibility when using SD-WAN connectivity

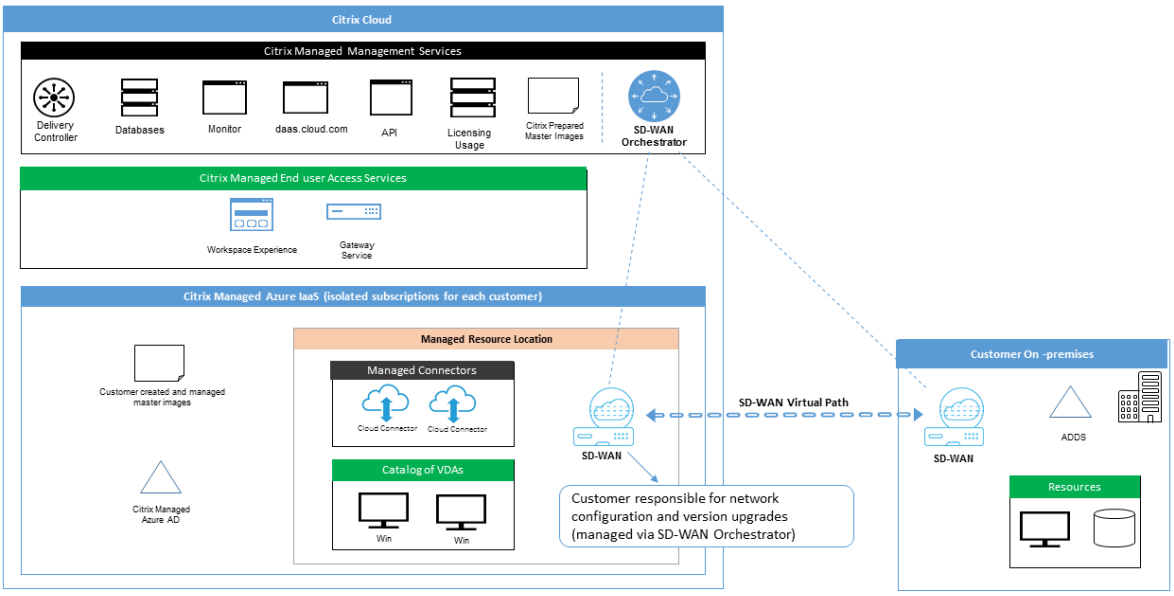
Citrix supports a fully automated way of deploying virtual Citrix SD-WAN instances to enable connectivity between Citrix DaaS for Azure and on-premises resources. Citrix SD-WAN connectivity has a number of advantages compared to VNet peering, including:

High reliability and security of VDA-to-datacenter and VDA-to-branch (ICA) connections.

- Best end-user experience for office workers, with advanced QoS capabilities and VoIP optimizations.
- Built-in ability to inspect, prioritize, and report on Citrix HDX network traffic and other application usage.

Citrix requires customers who want to take advantage of SD-WAN connectivity for Citrix DaaS for Azure to use SD-WAN Orchestrator for managing their Citrix SD-WAN networks.

The following diagram shows the added components in a Citrix DaaS for Azure deployment using SD-WAN connectivity.



The Citrix SD-WAN deployment for Citrix DaaS for Azure is similar to the standard Azure deployment configuration for Citrix SD-WAN. For more information, see Deploy Citrix SD-WAN Standard Edition Instance on Azure. In a high availability configuration, an active/standby pair of SD-WAN instances with Azure load balancers is deployed as a gateway between the subnet containing VDAs and Cloud Connectors, and the Internet. In a non-HA configuration, only a single SD-WAN instance is deployed as a gateway. Network interfaces of the virtual SD-WAN appliances are assigned addresses from a separate small address range split into two subnets.

When configuring SD-WAN connectivity, Citrix makes a few changes to the networking configuration of managed desktops described above. In particular, all outgoing traffic from the VNet, including traffic to Internet destinations, is routed through the cloud SD-WAN instance. The SD-WAN instance is also configured to be the DNS server for the Citrix-managed VNet.

Management access to the virtual SD-WAN instances requires an admin login and password. Each instance of SD-WAN is assigned a unique, random secure password that can be used by SD-WAN administrators for remote login and troubleshooting through the SD-WAN Orchestrator UI, the virtual appliance management UI and CLI.

Just like other tenant-specific resources, virtual SD-WAN instances deployed in a specific customer VNet are fully isolated from all other VNets.

When the customer enables Citrix SD-WAN connectivity, Citrix automates the initial deployment of virtual SD-WAN instances used with Citrix DaaS for Azure, maintains underlying Azure resources (virtual machines, load balancers, etc.), provides secure and efficient out-of-the-box defaults for the initial configuration of virtual SD-WAN instances, and enables ongoing maintenance and troubleshooting through SD-WAN Orchestrator. Citrix also takes reasonable measures to perform automatic validation

of SD-WAN network configuration, check for known security risks, and display corresponding alerts through SD-WAN Orchestrator.

Firewall policy for SD-WAN connections Citrix uses Azure firewall policies (network security groups) and public IP address assignment to limit access to network interfaces of virtual SD-WAN appliances:

- Only WAN and management interfaces are assigned public IP addresses and allow outbound connectivity to the Internet.
- LAN interfaces, acting as gateways for the Citrix-managed VNet, are only allowed to exchange network traffic with virtual machines on the same VNet.
- WAN interfaces limit inbound traffic to UDP port 4980 (used by Citrix SD-WAN for virtual path connectivity), and deny outbound traffic to the VNet.
- Management ports allow inbound traffic to ports 443 (HTTPS) and 22 (SSH).
- HA interfaces are only allowed to exchange control traffic with each other.

Access to infrastructure

Citrix may access the customer's Citrix-managed infrastructure (Cloud Connectors) to perform certain administrative tasks such as collecting logs (including Windows Event Viewer) and restarting services without notifying the customer. Citrix is responsible for executing these tasks safely and securely, and with minimal impact to the customer. Citrix is also responsible for ensuring any log files are retrieved, transported, and handled safely and securely. Customer VDAs cannot be accessed this way.

Backups for non-domain-joined catalogs

Citrix is not responsible for performing backups of non-domain-joined catalogs.

Backups for machine images

Citrix is responsible for backing up any machine images uploaded to Citrix DaaS for Azure, including images created with the image builder. Citrix uses locally redundant storage for these images.

Bastions for non-domain-joined catalogs

Citrix operations personnel have the ability to create a bastion, if necessary, to access the customer's Citrix-managed Azure subscription for diagnosing and repairing customer issues, potentially before the customer is aware of a problem. Citrix does not require the customer's consent to create a bastion. When Citrix creates the bastion, Citrix creates a strong randomly generated password for the

bastion and restricts RDP access to Citrix NAT IP addresses. When the bastion is no longer needed, Citrix disposes of it and the password is no longer valid. The bastion (and its accompanying RDP access rules) are disposed of when the operation completes. Citrix can access only the customer's non-domain-joined Cloud Connectors with the bastion. Citrix does not have the password to log in to non-domain-joined VDAs or domain-joined Cloud Connectors and VDAs.

Firewall policy when using troubleshooting tools

When a customer requests creation of a bastion machine for troubleshooting, the following security group modifications are made to the Citrix-managed VNet:

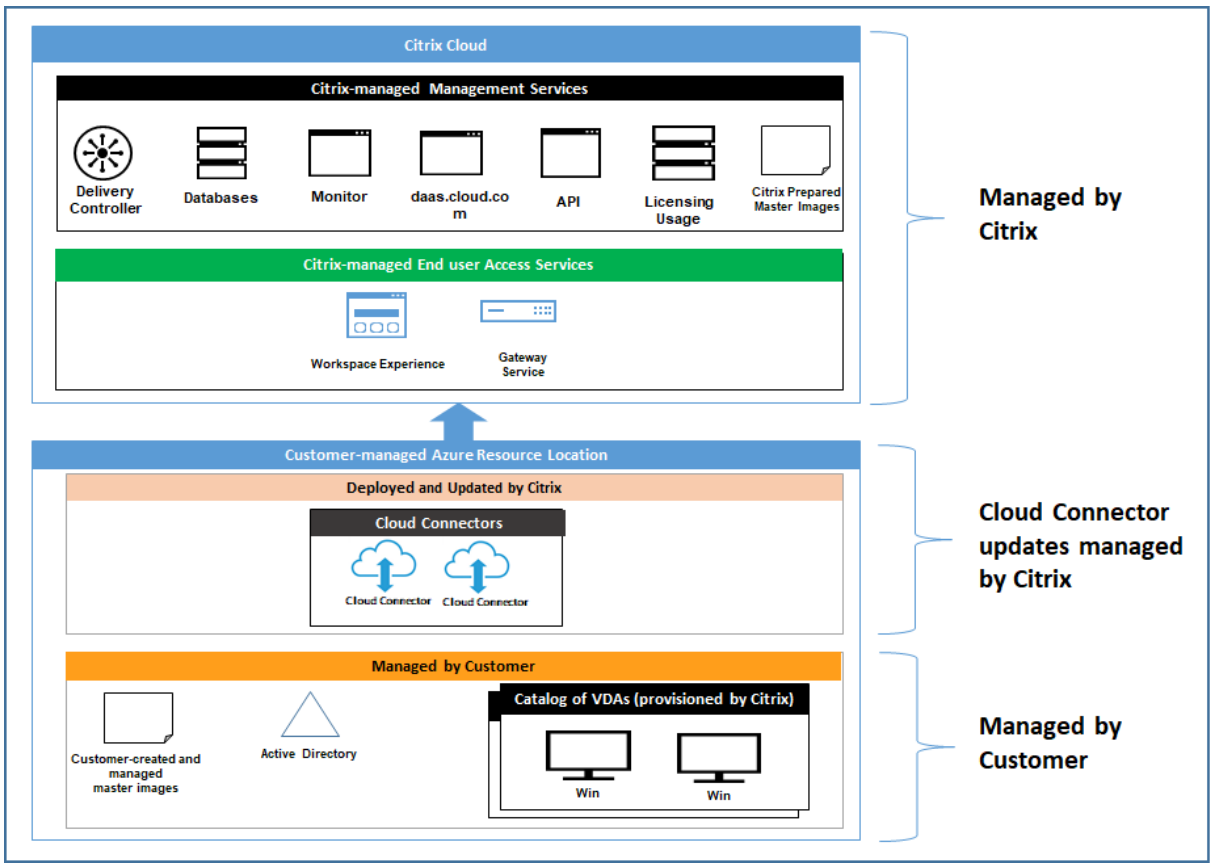
- Temporarily allow 3389 inbound from the customer-specified IP range to the bastion.
- Temporarily allow 3389 inbound from the bastion IP address to any address in the VNet (VDAs and Cloud Connectors).
- Continue to block RDP access between the Cloud Connectors, VDAs, and other VDAs.

When a customer enables RDP access for troubleshooting, the following security group modifications are made to the Citrix-managed VNet:

- Temporarily allow 3389 inbound from the customer-specified IP range to any address in the VNet (VDAs and Cloud Connectors).
- Continue to block RDP access between the Cloud Connectors, VDAs, and other VDAs.

Customer-managed subscriptions

For customer-managed subscriptions, Citrix adheres to the above responsibilities during deployment of the Azure resources. After deployment, everything above falls to the customer's responsibility, because the customer is the owner of the Azure subscription.



Customer responsibility

VDAs and machine images

The customer is responsible for all aspects of the software installed on VDA machines, including:

- Operating system updates and security patches
- Antivirus and antimalware
- VDA software updates and security patches
- Additional software firewall rules (especially outbound traffic)
- Follow Citrix security considerations and best practices

Citrix provides a prepared image that is intended as a starting point. Customers can use this image for proof-of-concept or demonstration purposes or as a base for building their own machine image. Citrix does not guarantee the security of this prepared image. Citrix will make an attempt to keep the operating system and VDA software on the prepared image up to date, and will enable Windows Defender on these images.

Customer responsibility when using VNet peering

The customer must open all ports specified in Customer-managed VNet with domain-joined machines.

When VNet peering is configured, the customer is responsible for the security of their own virtual network and its connectivity to their on-premises resources. The customer is also responsible for security of the incoming traffic from the Citrix-managed peered virtual network. Citrix does not take any action to block traffic from the Citrix-managed virtual network to the customer's on-premises resources.

Customers have the following options for restricting incoming traffic:

- Give the Citrix-managed virtual network an IP block which is not in use elsewhere in the customer's on-premises network or the customer-managed connected virtual network. This is required for VNet peering.
- Add Azure network security groups and firewalls in the customer's virtual network and on-premises network to block or restrict traffic from the Citrix-managed IP block.
- Deploy measures such as intrusion prevention systems, software firewalls, and behavioral analytics engines in the customer's virtual network and on-premises network, targeting the Citrix-managed IP block.

Customer responsibility when using SD-WAN connectivity

When SD-WAN connectivity is configured, customers have full flexibility to configure virtual SD-WAN instances used with Citrix DaaS for Azure according to their networking requirements, with the exception of a few elements required to ensure correct operation of SD-WAN in the Citrix-managed VNet. Customer responsibilities include:

- Design and configuration of routing and firewall rules, including rules for DNS and Internet traffic breakout.
- Maintenance of the SD-WAN network configuration.
- Monitoring of the operational status of the network.
- Timely deployment of Citrix SD-WAN software updates or security fixes. Since all instances of Citrix SD-WAN on a customer network must run the same version of SD-WAN software, deployments of updated software versions to Citrix DaaS for Azure SD-WAN instances need to be managed by customers according to their network maintenance schedules and constraints.

Incorrect configuration of SD-WAN routing and firewall rules, or mismanagement of SD-WAN management passwords, may result in security risks to both virtual resources in Citrix DaaS for Azure, and on-premises resources reachable through Citrix SD-WAN virtual paths. Another possible security risk stems from not updating Citrix SD-WAN software to the latest available patch release. While SD-WAN Orchestrator and other Citrix Cloud services provide the means to address such risks, customers are ultimately responsible for ensuring that virtual SD-WAN instances are configured appropriately.

Proxy

The customer may choose whether to use a proxy for outbound traffic from the VDA. If a proxy is used, the customer is responsible for:

- Configuring the proxy settings on the VDA machine image or, if the VDA is joined to a domain, using Active Directory Group Policy.
- Maintenance and security of the proxy.

Proxies are not allowed for use with Citrix Cloud Connectors or other Citrix-managed infrastructure.

Catalog resiliency

Citrix provides three types of catalogs with differing levels of resiliency:

- **Static:** Each user is assigned to a single VDA. This catalog type provides no high availability. If a user's VDA goes down, they will have to be placed on a new one to recover. Azure provides a 99.5% SLA for single-instance VMs. The customer can still back up the user profile, but any customizations made to the VDA (such as installing programs or configuring Windows) will be lost.
- **Random:** Each user is assigned randomly to a server VDA at launch time. This catalog type provides high availability via redundancy. If a VDA goes down, no information is lost because the user's profile resides elsewhere.
- **Windows 10 multisession:** This catalog type operates in the same manner as the random type but uses Windows 10 workstation VDAs instead of server VDAs.

Backups for domain-joined catalogs

If the customer uses domain-joined catalogs with a VNet peering, the customer is responsible for backing up their user profiles. Citrix recommends that customers configure on-premises file shares and set policies on their Active Directory or VDAs to pull user profiles from these file shares. The customer is responsible for the backup and availability of these file shares.

Disaster recovery

In the event of Azure data loss, Citrix will recover as many resources in the Citrix-managed Azure subscription as possible. Citrix will attempt to recover the Cloud Connectors and VDAs. If Citrix is unsuccessful recovering these items, customers are responsible for creating a new catalog. Citrix assumes that machine images are backed up and that customers have backed up their user profiles, allowing the catalog to be rebuilt.

In the event of the loss of an entire Azure region, the customer is responsible for rebuilding their customer-managed virtual network in a new region and creating a new VNet peering or a new SD-WAN instance within Citrix DaaS for Azure.

Citrix and customer shared responsibilities

Citrix Cloud Connector for domain-joined catalogs

Citrix DaaS for Azure deploys at least two Cloud Connectors in each resource location. Some catalogs may share a resource location if they are in the same region, VNet peering, and domain as other catalogs for the same customer. Citrix configures the customer's domain-joined Cloud Connectors for the following default security settings on the image:

- Operating system updates and security patches
- Antivirus software
- Cloud Connector software updates

Customers do not normally have access to the Cloud Connectors. However, they may acquire access by using catalog troubleshooting steps and logging in with domain credentials. The customer is responsible for any changes they make when logging in through the bastion.

Customers also have control over the domain-joined Cloud Connectors through Active Directory Group Policy. The customer is responsible for ensuring that the group policies that apply to the Cloud Connector are safe and sensible. For example, if the customer chooses to disable operating system updates using Group Policy, the customer is responsible for performing operating system updates on the Cloud Connectors. The customer can also choose to use Group Policy to enforce stricter security than the Cloud Connector defaults, such as by installing a different antivirus software. In general, Citrix recommends that customers put Cloud Connectors into their own Active Directory organizational unit with no policies, as this will ensure that the defaults Citrix uses can be applied without issue.

Troubleshooting

In the event the customer experiences problems with the catalog in Citrix DaaS for Azure, there are two options for troubleshooting: using bastions and enabling RDP access. Both options introduce security risk to the customer. The customer must understand and consent to undertaking this risk prior to using these options.

Citrix is responsible for opening and closing the necessary ports to carry out troubleshooting operations, and restricting which machines can be accessed during these operations.

With either bastions or RDP access, the active user performing the operation is responsible for the security of the machines that are being accessed. If the customer accesses the VDA or Cloud Connector through RDP and accidentally contracts a virus, the customer is responsible. If Citrix Support personnel access these machines, it is the responsibility of those personnel to perform operations safely. Responsibility for any vulnerabilities exposed by any person accessing the bastion or other machines in the deployment (for example, customer responsibility to add IP ranges to allow list, Citrix responsibility to implement IP ranges correctly) is covered elsewhere in this document.

In both scenarios, Citrix is responsible for correctly creating firewall exceptions to allow RDP traffic. Citrix is also responsible for revoking these exceptions after the customer disposes of the bastion or ends RDP access through Citrix DaaS for Azure.

Bastions Citrix may create bastions in the customer's Citrix-managed virtual network within the customer's Citrix-managed subscription to diagnose and repair issues, either proactively (without customer notification) or in response to a customer-raised issue. The bastion is a machine that the customer can access through RDP and then use to access the VDAs and (for domain-joined catalogs) Cloud Connectors through RDP to gather logs, restart services, or perform other administrative tasks. By default, creating a bastion opens an external firewall rule to allow RDP traffic from a customer-specified range of IP addresses to the bastion machine. It also opens an internal firewall rule to allow access to the Cloud Connectors and VDAs through RDP. Opening these rules poses a large security risk.

The customer is responsible for providing a strong password used for the local Windows account. The customer is also responsible for providing an external IP address range that allows RDP access to the bastion. If the customer elects not to provide an IP range (allowing anyone to attempt RDP access), the customer is responsible for any access attempted by malicious IP addresses.

The customer is also responsible for deleting the bastion after troubleshooting is complete. The bastion host exposes additional attack surface, so Citrix automatically shuts down the machine eight (8) hours after it is powered on. However, Citrix never automatically deletes a bastion. If the customer chooses to use the bastion for an extended period of time, they are responsible for patching and updating it. Citrix recommends that a bastion be used only for several days before deleting it. If the customer wants an up-to-date bastion, they can delete their current one and then create a new bastion, which will provision a fresh machine with the latest security patches.

RDP access For domain-joined catalogs, if the customer's VNet peering is functional, the customer can enable RDP access from their peered VNet to their Citrix-managed VNet. If the customer uses this option, the customer is responsible for accessing the VDAs and Cloud Connectors over the VNet peering. Source IP address ranges can be specified so RDP access can be restricted further, even within the customer's internal network. The customer will need to use domain credentials to log in to these machines. If the customer is working with Citrix Support to resolve an issue, the customer may need

to share these credentials with support personnel. After the issue is resolved, the customer is responsible for disabling RDP access. Keeping RDP access open from the customer's peered or on-premises network poses a security risk.

Domain credentials

If the customer elects to use a domain-joined catalog, the customer is responsible for providing to Citrix DaaS for Azure a domain account (username and password) with permissions to join machines to the domain. When supplying domain credentials, the customer is responsible for adhering to the following security principles:

- **Auditable:** The account should be created specifically for Citrix DaaS for Azure usage so that it is easy to audit what the account is used for.
- **Scoped:** The account requires only permissions to join machines to a domain. It should not be a full domain administrator.
- **Secure:** A strong password should be placed on the account.

Citrix is responsible for the secure storage of this domain account in an Azure Key Vault in the customer's Citrix-managed Azure subscription. The account is retrieved only if an operation requires the domain account password.

More information

For related information, see:

- Secure Deployment Guide for the Citrix Cloud Platform: Security information for the Citrix Cloud platform.
- Technical security overview: Security information for the Citrix DaaS
- Third party notifications

Subscribe to Citrix DaaS for Azure

October 12, 2022

Introduction

You can subscribe to Citrix DaaS Standard for Azure (formerly Citrix Virtual Apps and Desktops Standard for Azure service), and order the Citrix Azure Consumption Fund, through Citrix or through the Azure Marketplace. You can evaluate Citrix DaaS for Azure through Citrix.

If you currently subscribe to Citrix Virtual Apps Essentials or Citrix Virtual Desktops Essentials, you can upgrade to Citrix DaaS Standard for Azure.

A comprehensive order has two parts:

- **Citrix DaaS Standard for Azure:** Allows you to use your own (customer-managed) Azure subscriptions.
- **Citrix Azure Consumption Fund:** Further allows you to use a Citrix Managed Azure subscription, in addition to your own Azure subscriptions. Using a Citrix Managed Azure subscription offers the following benefits:
  - Single billing from Citrix, rather than billings from multiple companies.
  - Azure subscription feature differences.
  - Premium level Microsoft support through Citrix.

The Citrix Azure Consumption Fund isn't required. However, if you don't have it, you are restricted to using only your own Azure subscriptions, and you do not receive the other feature benefits.

The ordering process differs slightly, depending on the whether you order through Citrix or Azure Marketplace:

- When you order through Citrix, you can order Citrix DaaS Standard for Azure and the Citrix Azure Consumption Fund at the same time.
- When you order through Azure Marketplace, you first order Citrix DaaS Standard for Azure. Then, you order the Citrix Azure Consumption Fund.

  If you decide to order only Citrix DaaS for Azure, you can order the Citrix Azure Consumption Fund later, either through Azure Marketplace or through your Citrix account representative.

Regardless of where you order Citrix DaaS Standard for Azure and consumption fund, Citrix provides onboarding help. We'll also check to ensure that Citrix DaaS Standard for Azure is running and configured correctly.

Ordering summary

Summary of order steps:

1. Get a Citrix Cloud account.

   If you already have a Citrix Cloud account and currently subscribe to Citrix DaaS, see If you currently subscribe to Citrix DaaS.

2. Order Citrix DaaS Standard for Azure and consumption fund through Azure Marketplace, or order through Citrix.

Trials

Citrix DaaS Standard for Azure offers two types of trials:

- **Sales-approved:** In a sales-approved trial, you can use a Citrix Managed Azure subscription to create catalogs, images, and other tasks. From the trial, you can convert to a paid service subscription, and order the Citrix Managed Azure Consumption Fund. If you do not purchase consumption, any resources you created using the Citrix Managed Azure subscription are deleted automatically, which might affect users.
- **Auto-approved:** In an auto-approved trial, you can use your own (customer-managed) Azure subscription to create catalogs, images, and other tasks. From the trial, you can convert to a paid subscription. For more information, see Auto-approved service trials.

For more information about trials, see Citrix Cloud service trials.

Auto-approved service trials

- An auto-approved trial of Citrix DaaS Standard for Azure lasts 7 calendar days.
- During an auto-approved trial, you can create catalogs using your Azure subscription. Catalogs contain the machines that deliver desktops or applications.
- You can create catalogs using a Citrix-prepared image, an image you import from Azure, or an image you build in Citrix DaaS Standard for Azure.
- Users must be configured in an identity provider that Citrix Workspace supports.
- You can assign up to 25 users to catalogs in your trial deployment. Although you can assign a user to more than one catalog, a total of 25 unique named users are allowed in a trial deployment.
- You must have a Microsoft Azure user account, and at least one Azure subscription in that account. (Trials support only customer-owned (bring your own) Azure subscription use cases.)

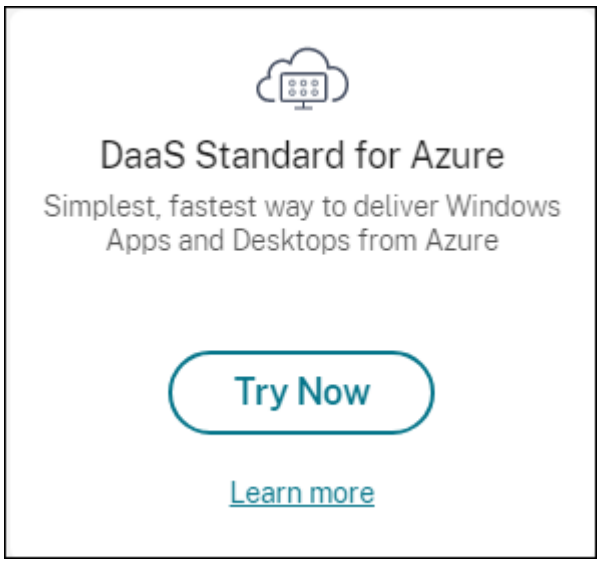
Request and use an auto-approved service trial

1. Sign up for a Citrix Cloud account (if you don't already have one).

   a) Browse to Citrix Cloud.
   b) Select **Sign up and try it free**.
   c) Follow the on-screen guidance.

   In a few moments, you'll receive an email about your Citrix Cloud account. Select the sign-in link in the email.

2. Request a trial. In the Citrix Cloud console, select **Try Now** on the **DaaS Standard for Azure** tile.



   You'll receive an email when your service trial is activated and ready (usually about two hours after you request the trial).

3. Sign in to Citrix Cloud.
4. Click **Manage** on the **DaaS Standard for Azure** tile.
5. Set up and configure your trial environment. During setup, you will:

   a) Add your Azure subscription to the service.
   b) Connect your identity provider through the Citrix Cloud console.
   c) Create a catalog.
   d) Add users from your identity provider to the catalog.
   e) Notify your users of the Citrix Workspace URL.

The graphical interface guides you through the setup process. For details, see the product documentation:

- Get acquainted with the product and its terminology.
- Review setup summaries and details.

Get a Citrix Cloud account

To sign up for a Citrix Cloud account and request a trial, go to https://onboarding.cloud.com. For details about that process, see Sign up for Citrix Cloud. Your account has an Organization ID (OrgID) that always appears in the upper right corner of the Citrix Cloud console.

Next steps: Order Citrix DaaS Standard for Azure through Citrix or through Azure Marketplace.

If you currently subscribe to Citrix DaaS

A Citrix Cloud account (OrgID) allows you to subscribe to only one edition of the Citrix DaaS at a time.

You can upgrade from Citrix DaaS Standard for Azure to either of the following editions:

- Citrix DaaS Advanced edition
- Citrix DaaS Premium edition.

Contact your Citrix representative for details.

If you currently subscribe to a Citrix DaaS edition other than Advanced or Premium (for example, Citrix Virtual Apps Essentials or Citrix Virtual Desktops Essentials), and want to subscribe to Citrix DaaS Standard for Azure, you must either:

- Subscribe to Citrix DaaS Standard for Azure using a different Citrix Cloud account (OrgID). For details, see Upgrade to Citrix DaaS Standard for Azure.
- Decommission the service you have, and then order Citrix DaaS Standard for Azure. For decommission instruction, see CTX239027.

You can use a Citrix Managed Azure subscription by purchasing the Citrix Azure Consumption Fund with any of the following service editions:

- Citrix DaaS Standard for Azure
- Citrix DaaS Advanced
- Citrix DaaS Advanced Plus
- Citrix DaaS Premium

Order through Citrix

You can order Citrix DaaS Standard for Azure (including the consumption fund) through Citrix Cloud, or through your Citrix account representative.

Through Citrix Cloud:

1. Sign in to Citrix Cloud. Click **Try Now** on the **DaaS Standard for Azure** tile. Complete the requested information. The text on the tile changes to **Trial Requested**.
2. Citrix contacts you. When Citrix DaaS Standard for Azure is available for you to use, the text on the tile changes to **Manage**.
3. Sign in to Citrix Cloud. On the **DaaS Standard for Azure** tile, click **Manage**. The first time you access Citrix DaaS Standard for Azure, you're taken to the Quick Deploy **Welcome** page.

Cancel a monthly subscription through Citrix

Monthly subscriptions renew automatically at the beginning of each month. You can use the Citrix DaaS Standard for Azure dashboard to cancel a monthly subscription that you ordered through Citrix.

(You cannot use Citrix DaaS Standard for Azure dashboard to cancel other subscription types that you ordered through Citrix, or orders placed through Azure Marketplace.)

To cancel a monthly subscription:

1. Sign in to Citrix Cloud.
2. In the upper left menu, select **My Services > DaaS Standard for Azure**.
3. From the **Manage > Azure Quick Deploy** dashboard, expand **General** on the right.
4. Click **Cancel Subscription**.
5. Your active resources are listed, such as catalogs, images, and connections. The page outlines the actions Citrix takes during a cancellation. It also informs you of actions you must take, if any. Indicate why you're canceling the service. Optionally, provide more feedback. When you're done, click **Cancel Subscription**.
6. Confirm that you understand the terms of the cancellation.

A banner on Citrix DaaS Standard for Azure dashboard indicates receipt of your cancellation request.

If you cancel your subscription accidentally, contact your Citrix sales representative or Citrix partner before the end of the month to reactivate Citrix DaaS Standard for Azure.

Order through Azure Marketplace

Order the Citrix DaaS Standard for Azure first, then order the Citrix Azure Consumption Fund.

You cannot order the consumption fund unless you previously purchased Citrix DaaS Standard for Azure. You cannot combine Citrix DaaS Standard for Azure and consumption fund in one order.

Citrix DaaS Standard for Azure is not offered through the Azure Cloud Solutions Providers portal. If you are a priority support customer, or interested in priority support, contact your Citrix account representative.

Requirements:

- The OrgID from your Citrix Cloud account.
  - If you have a Citrix Cloud account, but don't know the OrgID, look in the upper right corner of the Citrix Cloud console. Or, look at the email you received when you created the account.
  - If you don't have a Citrix Cloud account, follow the guidance in Get a Citrix Cloud account.
- An Azure account and at least one Azure subscription in that account.

Order Citrix DaaS Standard for Azure through Azure Marketplace

1. Sign in to the Azure Marketplace using your Azure account credentials.
2. Search for and then navigate to **Citrix DaaS Standard for Azure**.
3. Click **GET IT NOW**.
4. On the **One more thing** message, enable the check box and then click **Continue**.
5. The tabs contain information about the product, plans, pricing, and usage. When you're ready, select a plan (if more than one is available), and then click **Set up + subscribe**.
6. On the **Basics** tab:
   - **Subscription**: Indicates the plan that you selected.
   - **Name**: Enter a name for your subscription order.
   - The **Plan** section shows the price for the selected plan, based on monthly and multi-year (annual) terms.

     To change the plan term (monthly or annual), select **Change plan**. Select the term you want and click **Change plan**.
7. On the **Review + subscribe** tab:
   - Review the contact details you provided earlier for the Azure basic profile. You can change your address, phone number, or both.
   - Click **Subscribe**.
8. On the **Subscription in progress** page, click **Configure account now**. (If the button is disabled, wait a moment.) You're taken to a Citrix activation page.
9. On the activation page:
   - Use the **Sign in** link to sign in to Citrix Cloud. A successful sign-in automatically populates the **Organization ID** field.
   - **Quantity:** Enter the number of users. (An initial order must be at least 25.) An estimated price is displayed.
   - Agree to the terms and conditions, and then click **Activate Order**.

Citrix sends you an email when your service is provisioned. Provisioning can take a while. If you don't receive the email by the following day, contact Citrix Support.

When you receive the email from Citrix, you can begin using Citrix DaaS Standard for Azure. Remember: With only Citrix DaaS Standard for Azure, you can use only your own Azure subscriptions.

Do not delete the Citrix DaaS Standard for Azure resource in Azure. Deleting that resource cancels your subscription.

Order the consumption fund through Azure Marketplace

1. Sign in to the Azure Marketplace using your Azure account credentials.
2. Search for and then navigate to **Citrix Azure Consumption Fund**.
3. Click **GET IT NOW**.
4. Click **Set up + subscribe**.
5. On the **Subscribe** page:
   - In **Name**, enter an easily recognizable name, such as "My Managed Desktops."You can use this name later, if you want to change the service subscription.
   - Indicate how many users you want to support, in the range 25–100000.
   - Enter your email address and telephone number.

   When you're done, click **Subscribe**.
6. On the **Subscription progress** page, when the **Configure SaaS account on publisher's site** button becomes active (blue), click it. You're automatically directed to a Citrix order activation page.
7. On the Citrix order activation page, enter your Citrix Cloud OrgID. The email address you entered earlier is shown. You can change it, if needed. When you're done, click **Activate Order**.
8. Fulfillment of the consumption fund order does not take much time. When Citrix is notified of the order, a banner appears in the Citrix DaaS for Azure console, indicating that a Citrix Managed Azure subscription is being prepared for you.

   The **Cloud Subscriptions** panel on the right of the **Manage > Azure Quick Deploy** dashboard indicates when that subscription is ready for use.

Increase or decrease user seats through Azure Marketplace

If you need to increase user seats, create a new Azure Marketplace order for the additional number of seats you want.

To reduce the number of seats you have, cancel Citrix DaaS Standard for Azure in the Azure Marketplace, and then place an order for the desired number of seats.

Cancel Citrix DaaS Standard for Azure or consumption fund through Azure Marketplace

To cancel Citrix DaaS Standard for Azure or the consumption fund through Azure Marketplace:

1. Sign in to the Azure Marketplace.

2. Search for **DaaS**.
3. Select **New > View**.
4. Select the resource that you want to cancel.
5. In the resource's ellipsis menu, select **Delete**.
6. Click **Yes** in the confirmation box to acknowledge that you know the refund policy and want to cancel the resource.

> **Important:**
>
> Do not cancel the Citrix Azure Consumption Fund if you are using Citrix-managed resources, such as catalogs or images created in the Citrix Managed Azure subscription.

When your order is approved and processed

After your trial or service is approved, several tiles appear on the Citrix Cloud home page:

- Citrix DaaS for Azure
- Citrix DaaS
- Gateway

Citrix DaaS for Azure is the only service that is activated for your use.

To get started with Citrix DaaS Standard for Azure, sign in to Citrix Cloud. Access Citrix DaaS Standard for Azure using one of the following methods:

- On the **DaaS Standard for Azure** tile, click **Manage**.
- In the upper left menu, select **My Services > DaaS Standard for Azure**.

For setup guidance, see Get started.

Upgrade to Citrix DaaS Standard for Azure

If you currently subscribe to the Citrix Virtual Apps Essentials or Citrix Virtual Desktops Essentials service, upgrade to Citrix DaaS Standard for Azure by completing the following tasks.

1. Create a new Organizational ID (OrgID) to use with the Citrix DaaS Standard for Azure at https://onboarding.cloud.com/. (As described earlier in this article, you cannot use the same OrgID to subscribe to more than one Citrix DaaS edition.)
2. Contact Citrix Sales to purchase Citrix DaaS Standard for Azure and the Citrix Azure Consumption Fund, using the new OrgID. (You're not required to order the consumption fund, but without it, you can't access all the Citrix DaaS Standard for Azure features.)
3. Sign in to Citrix Cloud. In the upper left menu, select **My Services > DaaS Standard for Azure**.
4. Add at least one of your Azure subscriptions to Citrix DaaS Standard for Azure.

5. Import one or more images from your Azure subscriptions intoCitrix DaaS Standard for Azure.
6. Create catalogs, using the images you imported from your Azure subscriptions.
7. Add users to the catalogs you created.
8. If you want to keep the same Workspace URL you used with Citrix Virtual Apps Essentials or Citrix Virtual Desktops Essentials:

   a) Sign in to Citrix Cloud using the OrgID you use with the Essentials service. Select **Workspace Configuration** in the upper left menu. Change your Workspace URL to something different.
   b) Sign in to Citrix Cloud using the OrgID you use with the Citrix DaaS Standard for Azure. Select **Workspace Configuration** in the upper left menu. Change the Workspace URL to the one you formerly used for the Essentials service.

9. Sign in to Azure and delete all the resources you used with the Essentials service. For guidance, see Cancel Virtual Apps Essentials. (The procedure is equivalent for Citrix Virtual Desktops Essentials.)
10. Stop your Essentials service by deleting your Azure Marketplace resource in Azure.

Get started

August 30, 2022

This article summarizes the setup tasks for delivering desktops and apps using Citrix Daas Standard for Azure (formerly Citrix Virtual Apps and Desktops Standard for Azure service). We recommend that you review each procedure before actually doing it, so you know what to expect.

For Remote PC Access setup tasks, see Remote PC Access.

> **Important:**
>
> To ensure that you get important information about Citrix Cloud and the Citrix services you subscribe to, make sure you can receive all email notifications. For example, Citrix sends monthly informational notification emails detailing your Azure consumption (usage).
>
> In the upper right corner of the Citrix Cloud console, expand the menu to the right of the customer name and OrgID fields. Select **Account Settings**. On the **My Profile** tab, select all entries in the **Email Notifications** section.

Setup task summary

The following sections of this article guide you through setup tasks:

1. Prepare for setup.
2. Set up a deployment, following the guidance in one of:
   - Quick proof of concept deployment
   - Production deployment
3. Provide the workspace URL to your users.

Prepare

- If you aren't familiar with catalogs, images, network connections, or Azure subscriptions, review the introductory concepts and terminology information.
- Read the security overview to learn and understand what you (the customer) and Citrix are responsible for.
- If you don't already have a Citrix Cloud account that can be used for this service, get one, and then sign up for the service.
- Review the system requirements.
- Review the setup steps: proof of concept or production.

Set up a quick proof of concept deployment

This procedure requires a Citrix Managed Azure subscription.

1. Create a catalog using quick create.
2. Add your users to the Managed Azure AD.
3. Add your users to the catalog.
4. Notify your users of the Workspace URL.

Set up a production deployment

1. If you're using your own Active Directory or Azure Active Directory to authenticate users, connect and set that method in Citrix Cloud.
2. If you're using domain-joined machines, verify that you have valid DNS server entries.
3. If you're using your own Azure subscription (instead of a Citrix Managed Azure subscription), import your Azure subscription.
4. Create or import an image. Although you can use one of the Citrix prepared images as-is in a catalog, they're intended primarily for proof of concept deployments.
5. If you're using a Citrix Managed Azure subscription, and want your users to be able to access items in your network (such as file servers), set up an Azure VNet peering or Citrix SD-WAN connection.

6. Create a catalog using custom create.
7. If you're creating a catalog of multi-session machines, add apps to the catalog, if needed.
8. If you're using the Citrix Managed Azure AD to authenticate your users, add users to the directory.
9. Add users to the catalog.
10. Notify your users of the Workspace URL.

After you set up the deployment, use the **Monitor** dashboard in Citrix DaaS for Azure to see desktop usage, sessions, and machines.

System requirements

For all deployments:

- **Citrix Cloud:** This service is delivered through the Citrix Cloud and requires a Citrix Cloud account to complete the onboarding process. For details, see Get a Citrix Cloud account.
- **Windows licensing:** Ensure that you are properly licensed for Remote Desktop Services to run either Windows Server workloads or Azure Virtual Desktop Licensing for Windows 10.

If you're using a Citrix Managed Azure subscription:

- **Azure subscriptions when using Azure VNet peering (optional):** If you plan to access resources (such as AD and other file shares) in your own Azure network using Azure VNet peer connections, you must have an Azure subscription.
- **Joining VDAs to Azure Active Directory (optional):** To join VDAs to a domain using Active Directory Group Policy, you must be an administrator with permission to perform that action in Active Directory. For details, see Customer responsibility.

Configuring connections to your corporate on-premises network has extra requirements.

- Any connection (Azure VNet peering or SD-WAN): Requirements for all connections.
- Azure VNet peering connections: VNet peering requirements and preparation.
- SD-WAN connections: SD-WAN connection requirements and preparation.

If you want to use your own Azure images when creating a catalog, those images must meet certain requirements before you import them to Citrix DaaS for Azure.

Additional information:

- Internet connectivity requirements: System and connectivity requirements.
- Resource limits in a service deployment: Limits.

Supported operating systems

When using a Citrix Managed Azure subscription:

- Windows 7 (VDA must be 7.15 LTSR with latest Cumulative Update)
- Windows 10 single-session
- Windows 10 multi-session
- Windows Server 2012 R2
- Windows Server 2016
- Windows Server 2019
- Windows Server 2022 (requires minimum VDA 2106)
- Red Hat Enterprise Linux and Ubuntu

When using a customer-managed Azure subscription:

- Windows 7 (VDA must be 7.15 LTSR with latest Cumulative Update)
- Windows 10 Enterprise single-session
- Windows 10 Enterprise Virtual Desktop multi-session
- Windows Server 2008 R2
- Windows Server 2012 R2
- Windows Server 2016
- Windows Server 2019
- Windows Server 2022 (requires minimum VDA 2106)
- Red Hat Enterprise Linux and Ubuntu

Workspace URL

After you create catalogs and assign users, notify users where to find their desktops and apps: the Workspace URL. The Workspace URL is the same for all catalogs and users.

From the **Manage > Azure Quick Deploy** dashboard, view the URL by expanding **User Access & Authentication** on the right.

You can change the first part of the Workspace URL in Citrix Cloud. For instructions, see Customize the workspace URL.

Get help

Review the Troubleshoot article.

If you still have problems with the service, open a ticket by following the instructions in How to Get Help and Support.

Create catalogs

September 21, 2022

When used for published desktops and apps, a catalog is a group of identical virtual machines. When you deploy desktops, the machines in the catalog are shared with selected users. When you publish applications, multi-session machines host applications that are shared with selected users.

> **Note:**
>
> For information about creating Remote PC Access catalogs, see Remote PC Access.

Machine types

A catalog can contain one of the following types of machines:

- **Static:** The catalog contains single-session static machines (also known as personal, dedicated, or persistent desktops). Static means that when a user starts a desktop, that desktop "belongs" to that user. Any changes that that user makes to the desktop are retained at logoff. Later, when that user returns to Citrix Workspace and starts a desktop, it is the same desktop.
- **Random:** The catalog contains single-session random machines (also known as non-persistent desktops). Random means that when a user starts a desktop, any changes that that user makes to that desktop are discarded after logoff. Later, when that user returns to Citrix Workspace and starts a desktop, it might or might not be the same desktop.
- **Multi-session:** The catalog contains machines with apps and desktops. More than one user can access each of those machines simultaneously. Users can launch a desktop or apps from their workspace. App sessions can be shared. Session sharing is not permitted between an app and a desktop.
  - When you create a multi-session catalog, you select the work load: light (such as data entry), medium (such as office apps), heavy (such as engineering), or custom. Each option represents a specific number of machines and sessions per machine, which yields the total number of sessions that the catalog supports.
  - If you select the custom work load, you then select from available combinations of CPUs, RAM, and storage. Type the number of machines and sessions per machine, which yields the total number of sessions that the catalog supports.

When deploying desktops, the static and random machine types are sometimes called "desktop types."

Ways to create a catalog

There are several ways to create and configure a catalog:

- **Quick create** is the fastest way to get started. You provide minimal information, and Citrix DaaS for Azure takes care of the rest. A quick create catalog is great for a test environment or proof of concept.
- **Custom create** allows more configuration choices than quick create. It's more suited to a production environment than a quick create catalog.
- **Remote PC Access** catalogs contain existing machines (usually physical) that users access remotely. For details and instructions about these catalogs, see Remote PC Access.

Here's a comparison of quick create and custom create:

Quick create	Custom create
Less information to provide.	More information to provide.
Fewer choices for some features.	More choices for some features.
Citrix-managed Azure Active Directory user authentication.	Choice of: Citrix-managed Azure Active Directory, or your Active Directory/Azure Active Directory.
No connection to your on-premises network.	Choice of: No connection to your on-premises network, Azure VNet peering, and SD-WAN.
Uses a Citrix prepared Windows 10 image. That image contains a current desktop VDA.	Choice of: Citrix prepared images, your images that you import from Azure, or images you've built in Citrix DaaS for Azure from a Citrix prepared or imported image.
Each desktop has Azure standard disk (HDD) storage.	Several storage options are available.
Static desktops only.	Static, random, or multi-session desktops.
A power management schedule cannot be configured during creation. The machine hosting the desktop powers off when the session ends. (You can change this setting later.)	A power management schedule can be configured during creation.
Must use a Citrix Managed Azure subscription.	Can use the Citrix Managed Azure or your own Azure subscription.

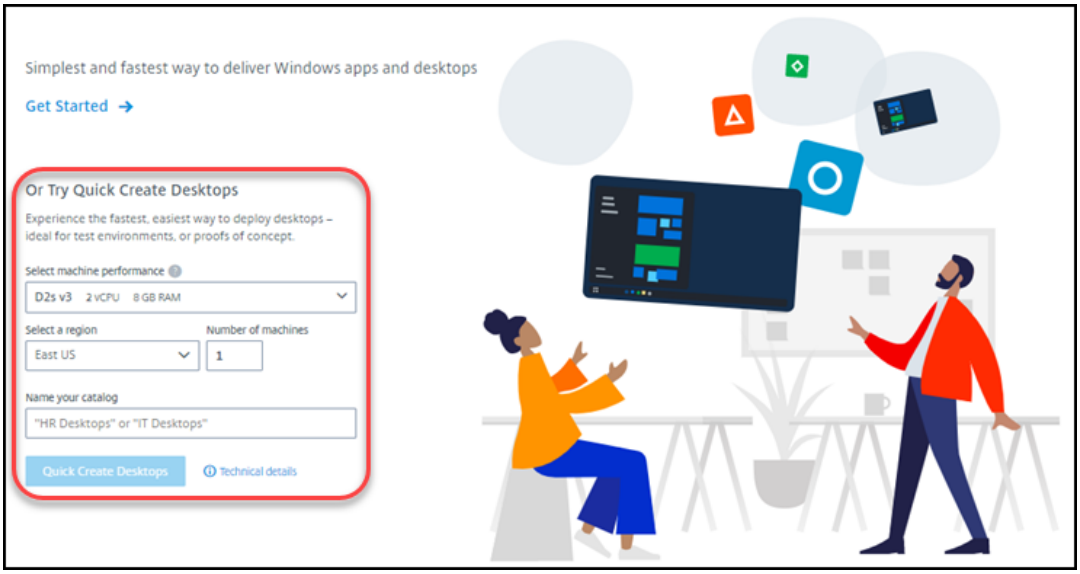
For details, see:

- Create a catalog using quick create
- Create a catalog using custom create

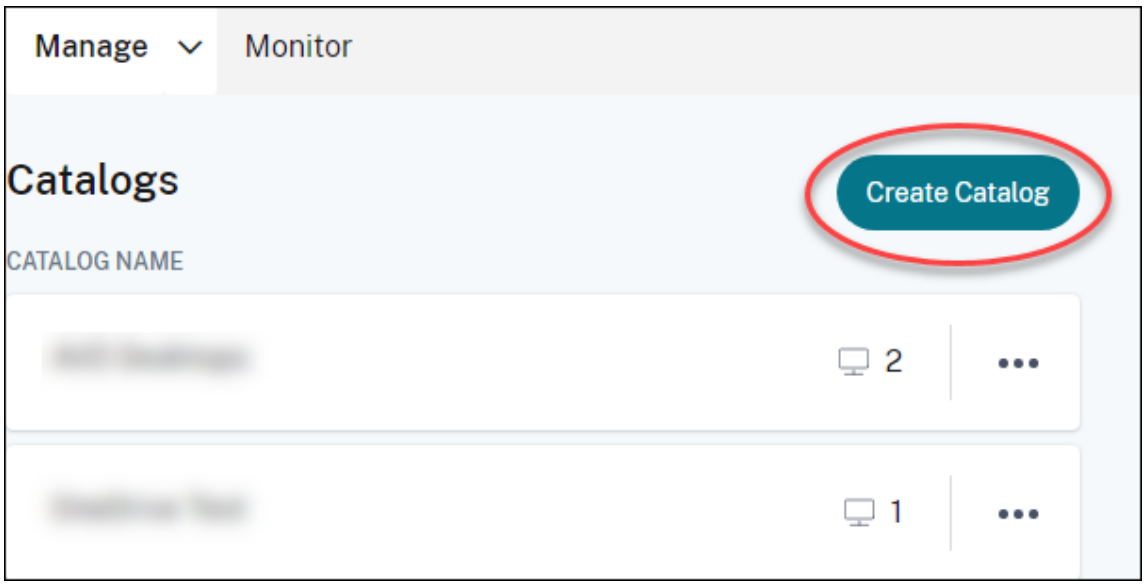
Create a catalog using quick create

This catalog creation method always uses a Citrix Managed Azure subscription.

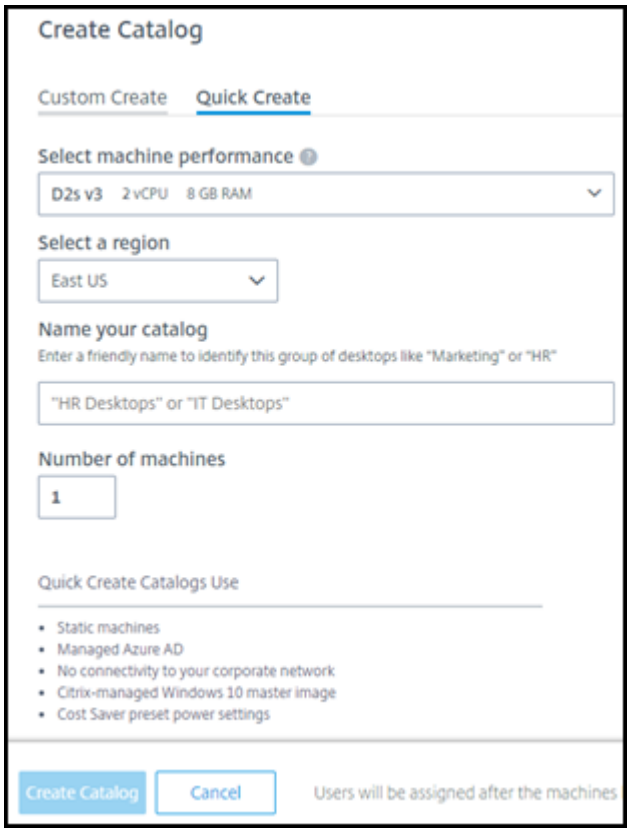
1. Sign in to Citrix Cloud.
2. In the upper left menu, select **My Services > DaaS Standard for Azure**.
3. If a catalog has not yet been created, you're taken to the Quick Deploy **Welcome** page. Choose one of:
   - Configure the catalog on this page. Continue with steps 6 through 10.



   - Click **Get Started**. You're taken to the **Manage > Azure Quick Deploy** dashboard. Click **Create Catalog**.
4. If a catalog has already been created (and you're creating another one), you're taken to the **Manage > Azure Quick Deploy** dashboard. Click **Create Catalog**.



5. Click **Quick Create** at the top of the page, if it is not already selected.



- **Machine performance:** Select the machine type. Each choice has a unique combination of CPUs, RAM, and storage. Higher-performance machines have higher monthly costs.
- **Region:** Select a region where you want the machines created. You might select a region that's close to your users.
- **Name:** Type a name for the catalog. This field is required, and there is no default value.

- **Number of machines:** Type the number of machines you want.

6. When you're done, click **Create Catalog**. (If you're creating the first catalog from the Quick Deploy **Welcome** page, click **Quick Create Desktops**.)

You're taken automatically to the **Manage > Azure Quick Deploy** dashboard. While the catalog is being created, the catalog's name is added to the list of catalogs, indicating its progress through creation.

Citrix DaaS for Azure also automatically creates a resource location and adds two Cloud Connectors.

What to do next:

- If you're using the Citrix Managed Azure AD for user authentication, you can add users to the directory while the catalog is being created.
- Regardless of which user authentication method you use, after the catalog is created, add users to the catalog.

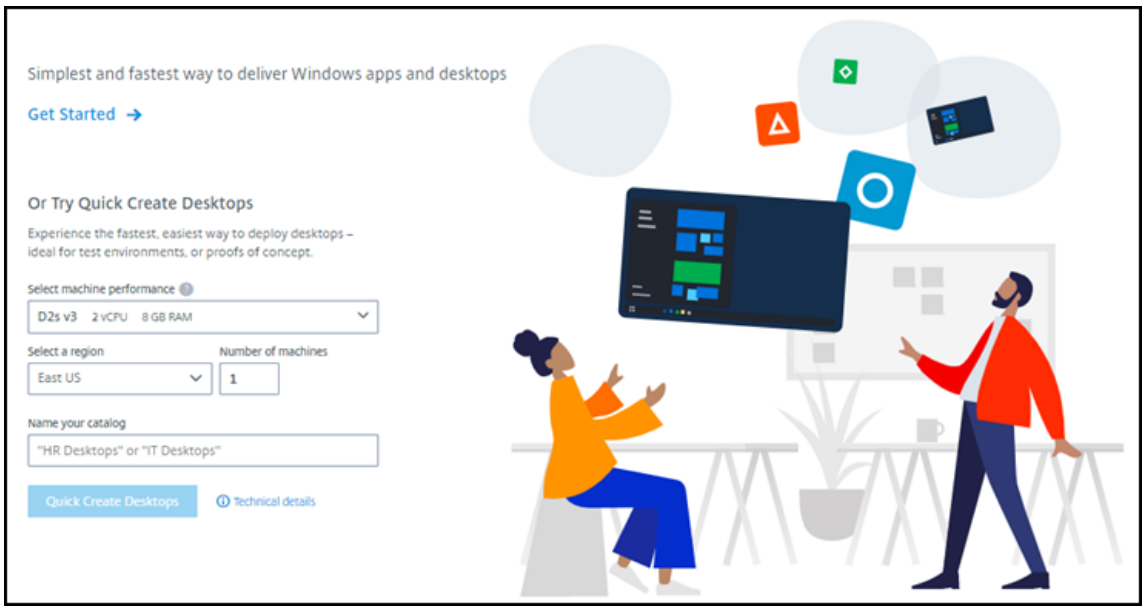
Create a catalog using custom create

If you are using a Citrix Managed Azure subscription, and plan to use a connection to your on-premises network resources, create that network connection before creating the catalog. To allow your users access to your on-premises or other network resources, you also need Active Directory information for that location.

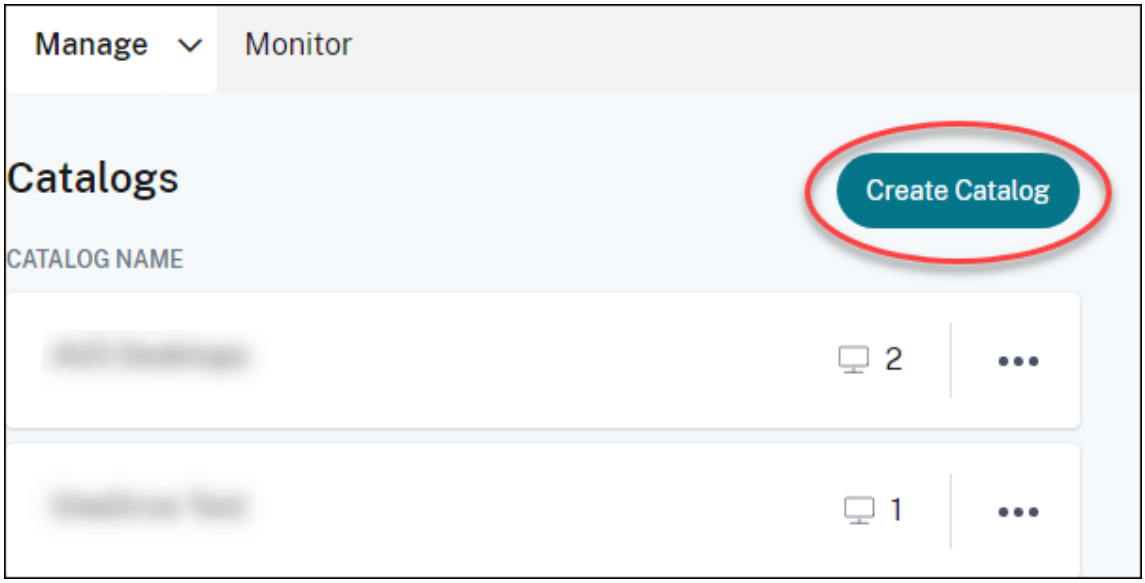
If you do not have a Citrix Managed Azure subscription, you must import (add) at least one of your own Azure subscriptions to Citrix DaaS for Azure before creating a catalog.

To create a catalog:

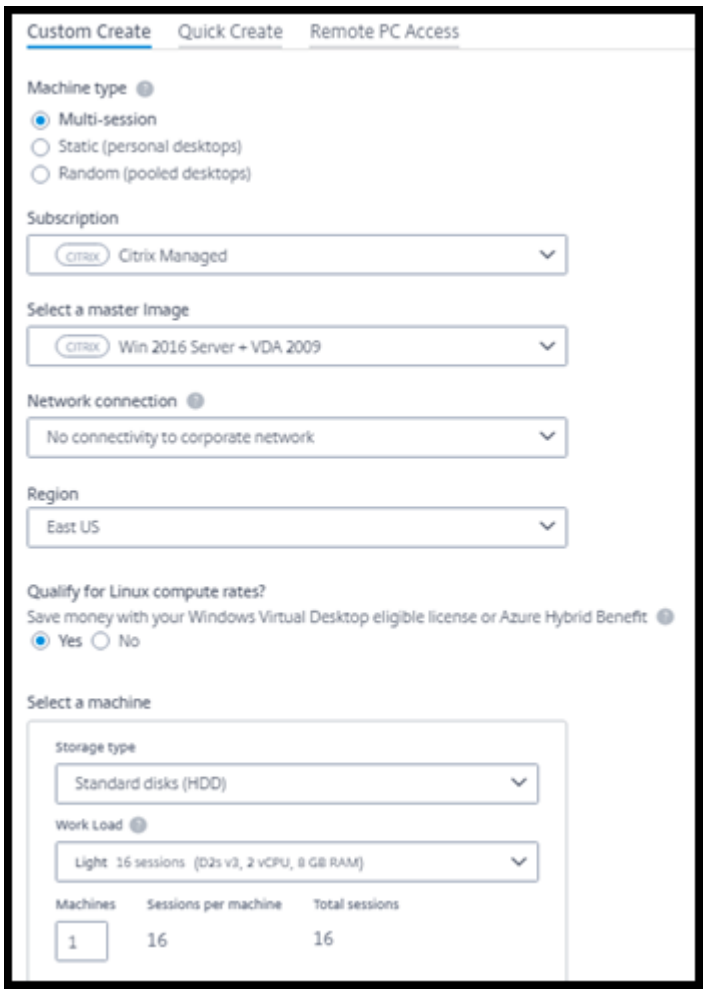
1. Sign in to Citrix Cloud.
2. In the upper left menu, select **My Services > DaaS Standard for Azure**.
3. If a catalog has not yet been created, you're taken to the Quick Deploy **Welcome** page. Click **Get Started**. At the end of the introduction page, you're taken to the **Manage > Azure Quick Deploy** dashboard. Click **Create Catalog**.



If a catalog has already been created, you're taken to the **Manage > Azure Quick Deploy** dashboard. Click **Create Catalog**.



4. Select **Custom Create** at the top of the page, if it's not already selected.



5. Complete the following fields. (Some fields are valid only for certain machine types. The field order might differ.)

   - **Machine type**. Select a machine type. For details, see Machine types.
   - **Subscription**. Select an Azure subscription. For details, see Azure subscriptions.
   - **Master image:** Select an operating system image. For details, see Images.
   - **Network connection:** Select the connection to use for accessing resources in your network. For details, see Network connections.
     - For a Citrix Managed Azure subscription, the choices are:
       - **No Connectivity:** Users cannot access locations and resources on your on-premises corporate network.
       - *Connections:* Select a connection, such as a VNet peering or SD-WAN connection.
     - For a customer-managed Azure subscription, select the appropriate resource group, virtual network, and subnet.

- **Region:** (Available only if you selected **No Connectivity** in **Network connection**.) Select a region where you want the desktops created. You might select a region that's close to your users.

  If you selected a connection name in **Network connection**, the catalog uses that network's region.

- **Qualify for Linux compute rates?** (Available only if you selected a Windows image.) You can save money when you use your eligible license or Azure Hybrid Benefit.

  Azure Virtual Desktop benefit: Eligible Windows 10 or Windows 7 per user licenses for:

  - Microsoft 365 E3/ES
  - Microsoft 365 A3/AS/Student Use Benefits
  - Microsoft 365 F3
  - Microsoft 365 Business Premium
  - Windows 10 Enterprise E3/E5
  - Windows 10 Education A3/A5
  - Windows 10 VDA per user

  Per user or per device license of RDS CAL with Software Assurance for Windows Server workloads.

  Azure Hybrid benefit: Windows Server licenses with active Software Assurance or the equivalent qualifying subscription licenses. See https://azure.microsoft.com/en-us/pricing/hybrid-benefit/.

- **Machine:**

  - **Storage type**. Standard disk (HDD), standard SSD, or premium SSD.
  - **Machine performance** (for **Static** or **Random** machine type), or **Workload** (for multi-session machine type). Choices include only options that match the generation type (gen1 or gen2) of the image you selected.

    If you select the custom work load, type the number of machines and sessions per machine in the **Machine Performance** field.

  - **Machines**. How many machines you want in this catalog.

- **Machine naming scheme:** see Machine naming scheme.
- **Name:** Type a name for the catalog. This name appears on the **Manage** dashboard.
- **Power schedule:** By default, the **I'll configure this later** check box is selected. For details, see Power management schedules.

6. When you're done, click **Create Catalog**.

The **Manage > Azure Quick Deploy** dashboard indicates when your catalog is created. Citrix DaaS for Azure also automatically creates a resource location and adds two Cloud Connectors.

What to do next:

- If you haven't done it already, configure the authentication method for your users to authenticate to Citrix Workspace.
- After the catalog is created, add users to the catalog.
- If you created a multi-session catalog, add applications (before or after adding users).

Creating catalogs of Azure AD domain-joined machines

You can use custom create to create catalogs of machines joined to your Azure Active Directory.

Requirements

Your deployment must include Citrix Cloud Connectors. Machine Creation Services deploys your Cloud Connectors based on the information you provide about you Azure AD domain when you create a catalog.

This type of catalog can only be used to provision static or random machines. Provisioning of multi-session machines is not supported at this time.

Don't join the master image to Azure AD before creating a catalog. Citrix MCS joins the master image to Azure AD when the catalog is created.

Use VDA version 2203 or higher.

In the Azure portal, assign the Virtual Machine User Login IAM role to the virtual machines in the catalog. You can do this in several ways:

- Most secure: If you are creating static machines, assign the role to the user assign to the machine.
- Alternate method: Assign the role on the resource groups containing the virtual machines, to all users with access to the catalog.
- Least secure: Assign the role on the subscriptions, to all users with access to the catalog.

Set Workspace authentication to use the Azure AD you are joining to the machines in the catalog. For instructions, see Configure user authentication in Citrix Cloud.

For more information about requirements, known issues, and considerations, see the information about pure Azure AD joined VDA configurations in Azure Active Directory joined and non-domain joined VDA configuration.

To create a catalog

1. Sign in to Citrix Cloud.
2. In the upper left menu, select **My Services > DaaS Standard for Azure**.
3. Select **Manage > Azure Quick Deploy**.
4. If a catalog has not yet been created, you're taken to the **Welcome** page. Select **Get Started**. At the end of the introduction page, you're taken to the **Manage > Azure Quick Deploy** dashboard. Select **Create Catalog**. If a catalog has already been created, you're taken to the **Manage > Azure Quick Deploy** dashboard. Select **Create Catalog**.
5. Select **Custom Create** at the top of the page, if it's not already selected.
6. Complete the following fields.
   - **Machine type.** Select **Static (personal desktops)** or **Random (pooled desktops)**.
   - **Subscription**. Select your Azure subscription.
   - **Master image.** Select an operating system image to be used for the machines in the catalogs.
   - **Network connection.** Select the appropriate resource group, virtual network, and subnet.
   - **Domain configuration**. Select **Azure Active Directory** as your domain type. A warning might appear reminding you to set Workspace authentication use this Azure AD.
7. Complete the remainder of the wizard to create the catalog.

Resource location settings when creating a catalog

When creating a catalog, you can optionally configure several resource location settings.

When you click **Advanced settings** in the Quick Deploy catalog creation dialog, Citrix DaaS for Azure retrieves resource location information.

- If you already have a resource location for the domain and network connection selected for the catalog, you can save it for use by the catalog you're creating.

  If that resource location has only one Cloud Connector, another one is installed automatically. You can optionally specify advanced settings for the Cloud Connector you're adding.

- If you don't have a resource location set up for the domain and network connection selected for the catalog, you're prompted to configure one.

Configure advanced settings:

- (Required only when the resource location is already set up.) A name for the resource location.
- External connectivity type: through the Citrix Gateway service, or from within your corporate network.

- Cloud Connector settings:
  - (Available only when using a customer-managed Azure subscription) Machine performance. This selection is used for the Cloud Connectors in the resource location.
  - (Available only when using a customer-managed Azure subscription) Azure resource group. This selection is used for the Cloud Connectors in the resource location. The default is the resource group last used by the resource location (if applicable).
  - Organizational Unit (OU). The default is the OU last used by the resource location (if applicable).

When you're done with the advanced settings, click **Save** to return to the Quick Deploy catalog creation dialog.

After you create a catalog, several resource location actions are available. For details, see Resource location actions.

Machine naming scheme

To specify a machine naming scheme when creating a catalog using Quick Deploy, select **Specify machine naming scheme**. Use from 1-4 wildcards (hash marks) to indicate where sequential numbers or letters appear in the name. Rules:

- The naming scheme must contain at least one wildcard, but not more than four wildcards. All the wildcards must be together.
- The entire name, including wildcards, must be between 2 and 15 characters.
- A name cannot include blanks (spaces), slashes, backslashes, colons, asterisks, angle brackets, pipes, commas, tildes, exclamation points, at signs, dollar signs, percent signs, carets, parentheses, braces, or underscores.
- A name cannot begin with a period.
- A name cannot contain only numbers.
- Do not use the following letters at the end of a name: `-GATEWAY`, `-GW`, and `-TAC`.

Indicate whether the sequential values are numbers (0-9) or letters (A-Z).

For example, a naming scheme of `PC-Sales-##` (with **0-9** selected) results in computer accounts named `PC-Sales-01`, `PC-Sales-02`, `PC-Sales-03`, and so on.

Leave enough room for growth.

- For example, a naming scheme with 2 wildcards and 13 other characters (for example, `MachineSales-##`) uses the maximum number of characters (15).
- Once the catalog contains 99 machines, the next machine creation fails. The service tries to create a machine with three digits (100), but that would create a name with 16 characters. The maximum is 15.

- So, in this example, a shorter name (for example, `PC-Sales-##`) allows scaling beyond 99 machines.

If you do not specify a machine naming scheme, Citrix DaaS for Azure uses the default naming scheme `DAS%%%%%-**-###`.

- %%%%% = five random alphanumeric characters matching the resource location prefix
- ** = two random alphanumeric characters for the catalog
- ### = three digits.

Related information

- Domain-joined and non-domain-joined machines.
- Remote PC Access catalogs.
- Create a catalog in a network that uses a proxy server.
- Display catalog information.

Remote PC Access

August 30, 2022

Introduction

> **Note:**
>
> This article describes how to configure Remote PC Access when using the Quick Deploy management interface in Citrix DaaS Standard for Azure (formerly Citrix Virtual Apps and Desktops Standard for Azure service). For information about configuring Remote PC Access when using the Full Configuration management interface, see Remote PC Access.

Citrix Remote PC Access enables users to remotely use physical Windows or Linux machines located in the office. Users receive the best user experience by using Citrix HDX to deliver their office PC session.

Remote PC Access supports domain-joined machines.

Differences from delivering virtual desktops and apps

If you're familiar with delivering virtual desktops and apps, the Remote PC Access feature has several differences:

- A Remote PC Access catalog usually contains existing physical machines. So, you don't have to prepare an image or provision machines to use Remote PC Access. Delivering desktops and apps usually uses virtual machines (VMs), and an image is used as a template to provision the VMs.
- When a machine in a Remote PC Access random pooled catalog is powered off, it is not reset to the original state of the image.
- For Remote PC Access static user assignment catalogs, the assignment occurs after a user logs in (either at the machine or via RDP). When delivering desktops and apps, a user is assigned if a machine is available.

Installation and configuration summary

Review this section before starting the tasks.

1. Before you start:

   a) Review the requirements and considerations.
   b) Complete the preparation tasks.

2. From Citrix Cloud:

   a) Set up a Citrix Cloud account and subscribe to the Citrix DaaS Standard for Azure service.

   b) Set up a resource location that can access your Active Directory resources. Install at least two Cloud Connectors in the resource location. The Cloud Connectors communicate with Citrix Cloud.

      Follow the guidance for creating a resource location and installing Cloud Connectors in it. This information includes system requirements, preparation, and procedures.

   c) Connect your Active Directory to Citrix Cloud.

3. Install a Citrix Virtual Delivery Agent (VDA) on each machine that users will access remotely. VDAs communicate with Citrix Cloud through the Cloud Connectors in the resource location.

4. From Citrix DaaS for Azure Quick Deploy management interface:

   a) Create a Remote PC Access catalog. In this procedure, you specify the location of your resource location and select the user assignment method.
   b) Add subscribers (users) to the catalog, if needed. Add users to a catalog if the catalog uses either the static autoassigned or random pooled user assignment method. You do not need to add users to a static preassigned catalog.

5. Send the workspace URL to users. From their workspace, users can log on to their machines in the office.

Requirements and considerations

References to machines in this section refer to the machines that users access remotely.

General:

- The machines must be running a single-session Windows 10 or Linux (Red Hat Enterprise Linux and Ubuntu) operating system.
- The machine must be joined to an Active Directory Domain Services domain.
- If you are familiar with using Remote PC Access with Citrix Virtual Apps and Desktops, the Wake-on-LAN feature is not available in Citrix DaaS for Azure.

Network:

- The machine must have an active network connection. A wired connection is preferred for greater reliability and bandwidth.
- If using Wi-Fi:
  - Set the power settings to leave the wireless adapter turned on.
  - Configure the wireless adapter and network profile to allow automatic connection to the wireless network before the user logs on. Otherwise, the VDA does not register until the user logs on. The machine isn't available for remote access until a user logs on.
  - Ensure that the Cloud Connectors can be reached from the Wi-Fi network.

Devices and peripherals:

- The following devices are not supported:
  - KVM switches or other components that can disconnect a session.
  - Hybrid PCs, including All-in-One and NVIDIA Optimus laptops and PCs.
  - Dual boot machines.
- Connect the keyboard and mouse directly to the machine. Connecting to the monitor or other components that can be turned off or disconnected, can make these peripherals unavailable. If you must connect the input devices to components such as monitors, do not turn those components off.
- For laptop and Surface Pro devices: Ensure that the laptop is connected to a power source instead of running on the battery. Configure the laptop power options to match the options of a desktop machine. For example:
  - Disable the hibernate feature.
  - Disable the sleep feature.
  - Set the close lid action to **Do Nothing**.
  - Set the *press the power button* action to **Shut Down**.

  - Disable video card and NIC energy-saving features.

When using a docking station, you can undock and redock laptops. When you undock the laptop, the VDA reregisters with the Cloud Connectors over Wi-Fi. However, when you redock the laptop, the VDA doesn't switch to use the wired connection until you disconnect the wireless adapter. Some devices provide built-in functionality to disconnect the wireless adapter upon establishing a wired connection. Other devices require custom solutions or third-party utilities to disconnect the wireless adapter. Review the Wi-Fi considerations mentioned previously.

To enable docking and undocking for Remote PC Access devices:

- In **Start > Settings > System > Power & Sleep**, set **Sleep** to **Never**.
- In **Device Manager > Network adapters > Ethernet adapter**, go to **Power Management** and clear **Allow the computer to turn off this device to save power**. Ensure that **Allow this device to wake the computer** is selected.

Linux VDA:

- Use the Linux VDA on physical machines only in non-3D mode. Due to limitations on NVIDIA's driver, the PC's local screen annot be blacked out, and displays session activities when HDX 3D mode is enabled. Showing this screen is a security risk.
- Catalogs with Linux machines must use the static preassigned user assignment method. Catalogs with Linux machines cannot use either the static autoassigned or random pooled assignment methods.

Workspace considerations:

- Multiple users with access to the same office PC see the same icon in Citrix Workspace. When a user signs in to Citrix Workspace, that machine appears as unavailable if it is already in use by another user.

Prepare

- Decide how to install the VDA on the machines. Several methods are available:
  - Manually install the VDA on each machine.
  - Push the VDA installation using Group Policy, using a script.
  - Push the VDA installation using an Electronic Software Distribution (ESD) tool such as Microsoft System Center Configuration Manager (SCCM). For details, see Install VDAs using SCCM.
- Learn about user assignment methods and decide which method you'll use. You specify the method when creating a Remote PC Access catalog.

- Decide how the machines (actually the VDAs you install on the machines) will register with Citrix Cloud. A VDA must register to establish communications with the session broker in Citrix Cloud.

  VDAs register through the Cloud Connectors in their resource location. You can specify Cloud Connector addresses when you install a VDA, or later.

  For a VDA's first (initial) registration, Citrix recommends using policy-based GPO or LGPO. After the initial registration, Citrix recommends using auto-update, which is enabled by default. Learn more about VDA registration.

Install a VDA

Download and install a VDA on each physical machine that users will access remotely.

Download a VDA

- To download a Windows VDA:

  1. Using your Citrix Cloud account credentials, browse to the Citrix DaaS download page.
  2. Download the latest VDA. Two types of installation packages are available. The year and month values in the VDA title vary.

- To download a Linux VDA for Remote PC Access, follow the guidance in the Linux VDA documentation.

Windows VDA installation package types The Citrix download site provides two Windows VDA installation package types that can be used for Remote PC Access machines:

- Single-session core VDA installer (*release* is *yymm*): `VDAWorkstationCoreSetup_release.exe`

  The single-session core VDA installer is tailored specifically for Remote PC Access. It's lightweight and easier to deploy (than other VDA installers) over the network to all machines. It does not include components that typically aren't needed in these deployments, such as Citrix Profile Management, Machine Identity Service, and the user personalization layer.

  However, without Citrix Profile Management installed, the displays for Citrix Analytics for Performance and some Monitor details aren't available. For details about those limitations, see the blog post Monitor and troubleshoot Remote PC Access machines.

  If you want full analytics and monitoring displays, use the single-session full VDA installer.

- Single-session full VDA installer (*release* is *yymm*): `VDAWorkstationSetup_release.exe`

Although the single-session full VDA installer is a larger package than the single-session core VDA installer, you can tailor it to install only the components you need. For example, you can install the components that support Profile Management.

Install a Windows VDA for Remote PC Access interactively

1. Double-click the VDA installation file that you downloaded.
2. On the **Environment** page, select **Enable Remote PC Access**, and then click **Next**.
3. On the **Delivery Controller** page, select one of the following:
   - If you know the addresses of your Cloud Connectors, select **Do it manually**. Enter the FQDN of a Cloud Connector and click **Add**. Repeat for the other Cloud Connectors in your resource location.
   - If you know where you installed the Cloud Connectors in your AD structure, select **Choose locations from Active Directory**, and then navigate to that location. Repeat for the other Cloud Connectors.
   - If you want to specify the Cloud Connector addresses in Citrix Group Policy, select **Do it later (Advanced)**, and then confirm that selection when prompted.

   When you're done, click **Next**.
4. If you're using the single-session full VDA installer, on the **Additional Components** page, select the components you want to install, such as Profile Management. (This page does not appear if you're using the single-session core VDA installer.)
5. On the **Features** page, click **Next**.
6. On the **Firewall** page, select **Automatically** (if it isn't already). Then click **Next**.
7. On the **Summary** page, click **Install**.
8. On the **Diagnose** page, click **Connect**. Make sure the check box is selected. When prompted, enter your Citrix account credentials. After your credentials are validated, click **Next**.
9. On the **Finish** page, click **Finish**.

For full installation information, see Install VDAs.

Install a Windows VDA for Remote PC Access using a command line

- If you're using the single-session core VDA installer: Run `VDAWorkstationCoreSetup.exe`, and include the `/quiet`, `/enable_hdx_ports`, and `/enable_hdx_udp_ports` options. To specify Cloud Connector addresses, use the `/controllers` option.

For example, the following command installs a single-session core VDA. Citrix Workspace app and other non-core services are not installed. The FQDNs of two Cloud Connectors are specified, and ports in the Windows Firewall Service will be opened automatically. The administrator will handle restarts.

```
VDAWorkstationCoreSetup .exe /quiet /controllers "Connector-East.domain.com"“Connector-East2.domain.com” /enable_hdx_ports /noreboot
```

- If you're using the single-session full VDA installer and want to include Profile Management (or other optional components): Run `VDAWorkstationSetup.exe` and include the `/remotepc` and `/includeadditional` options. The `/remotepc` option prevents installation of most optional components. The `/includeadditional` option specifies exactly which components you want to install.

  For example, the following command prevents installation of all optional additional components except Profile Management.

  ```
  VDAWorkstationSetup.exe /quiet /remotepc /includeadditional “Citrix User Profile Manager”,“Citrix User Profile Manager WMI Plugin” /controllers “connector.domain.com” “connector2.domain.com” /enable_hdx_ports /noresume /noreboot
  ```

For details, see Command-line options to install a VDA.

Install a Linux VDA

Follow the guidance in the Linux documentation for installing a Linux VDA interactively or using the command line.

Create a Remote PC Access catalog

A resource location containing at least two Cloud Connectors must exist before you can successfully create a catalog.

> **Important:**
>
> A machine can belong to only one catalog at a time. This restriction is not enforced when you specify the machines to be added to a catalog. However, ignoring the restriction can cause problems later.

1. Sign in to Citrix Cloud.
2. In the upper left menu, select **My Services > DaaS Standard for Azure**.

3. If you haven't created any catalogs yet, click **Get Started** on the Quick Deploy **Welcome** page. If you have created a catalog, click **Create Catalog** on the **Manage > Azure Quick Deploy** dashboard.
4. On the **Remote PC Access** tab, select a method for assigning users to machines.
5. Enter a name for the catalog and select the resource location you created.
6. Add machines.
7. Click **Create Catalog**.
8. On the **Your Remote PC Access catalog is being created** page, click **Done**.
9. An entry for the new catalog appears on the **Manage** dashboard.

   After the catalog is successfully created, click one of the links to add subscribers (users) to the catalog. This step applies if the catalog uses either the static autoassigned or random pool unassigned user assignment method.

After you create a catalog and add users (if needed), send the Workspace URL to your users.

User assignment methods

The user assignment method that you choose when creating a catalog indicates how users are assigned to machines.

- **Static autoassigned:** User assignment occurs when a user logs on to the machine (not using Citrix, for example, in-person or RDP), after a VDA is installed on the machine. Later, if other users log on to that machine (not using Citrix), they are also assigned. Only one user can use the machine at a time. This is a typical setup for either office workers or shift workers who share a computer.

  This method is supported for Windows machines. It cannot be used with Linux machines.

- **Static preassigned:** Users are preassigned to machines. (This is usually configured by uploading a CSV file containing machine-user mapping.) There is no need for user logon to establish assignment after the VDA is installed. There is also no need to assign users to the catalog after it's created. This is best for office workers.

  This method is supported for Windows and Linux machines.

- **Random pool unassigned:** Users are randomly assigned to an available machine. Only one user can use the machine at a time. This is ideal for computing labs in schools.

  This method is supported for Windows machines. It cannot be used with Linux machines.

Methods for adding machines to a catalog

Remember: Each machine must have a VDA installed on it.

When creating or editing a catalog, there are three ways you can add machines to a catalog:

- Select machine accounts one by one.
- Select OUs.
- Add in bulk using a CSV file. A template is available for you to use for the CSV file.

Add machine names

This method adds machine accounts one by one.

1. Select your domain.
2. Search for the machine account.
3. Click **Add**.
4. Repeat to add more machines.
5. When you finish adding machines, click **Done**.

Add OUs

This method adds machine accounts according to the Organizational Unit where they reside.
When selecting OUs, choose lower-level OUs for greater granularity. If that granularity is not required, you can choose higher-level OUs.

For example, in the case of `Bank/Officers/Tellers`, select `Tellers` for greater granularity. Otherwise, you can select `Officers` or `Bank`, based on the requirement.

Moving or deleting OUs after they're assigned to a Remote PC Access catalog affects VDA associations and causes issues with future assignments. Ensure that your AD change plan accounts for OU assignment updates for catalogs.

To add OUs:

1. Select your domain.
2. Select the OUs that contain the machines accounts you want to add.
3. Indicate in the check box whether to include subfolders included in your selections.
4. When you finish selecting OUs, click **Done**.

Add in bulk

1. Click **Download CSV Template**.

2. In the template, add the machine account information (up to 100 entries). The CSV file can also contain the names of users assigned to each machine.
3. Save the file.
4. Either drag the file on to the **Add machines in bulk** page or browse to the file.
5. A preview of the file's content is displayed. If that's not the file you want, you can create another file and then drag or browse to it.
6. When you're finished, click **Done**.

Manage Remote PC Access catalogs

To display or change a Remote PC Access catalog's configuration information, select the catalog from the **Manage > Azure Quick Deploy** dashboard (click anywhere in its entry).

- From the **Details** tab, you can add or remove machines.
- From the **Subscribers** tab, you can add or remove users.
- From the **Machines** tab, you can:
  - Add or remove machines: **Add or remove machines** button.
  - Change user assignments: **Remove assignment** trash icon, **Edit machine assignment** in ellipsis menu.
  - See which machines are registered, and place machines in or out of maintenance mode.

Azure subscriptions

August 9, 2023

Introduction

Citrix DaaS Standard for Azure (formerly Citrix Virtual Apps and Desktops Standard for Azure service) supports both Citrix Managed Azure subscriptions and your own, customer-managed Azure subscriptions.

- To use your own Azure subscriptions, you first import (add) one or more of those subscriptions to Citrix DaaS for Azure. That action enables Citrix DaaS for Azure to access your Azure subscriptions.
- Using a Citrix Managed Azure subscription requires no subscription configuration. However, to have a Citrix Managed Azure subscription available, you must have ordered the Citrix Azure Consumption Fund (in addition to the Citrix DaaS Standard for Azure).

When you create a catalog or build an image, you choose among the available Azure subscriptions.

Some service features differ, depending on whether the machines are in a Citrix Managed Azure subscription or in your own Azure subscription.

Citrix Managed Azure subscription	Your own Azure subscription
Supports domain-joined or non-domain-joined machines.	Supports only domain-joined machines.
Supports quick create and custom create catalogs.	Supports only custom create catalogs.
Always available (and is the default subscription selection) when creating catalogs and images.	Must add the Azure subscription to Citrix DaaS for Azure before creating a catalog.
For user authentication, supports Citrix Managed Azure Active Directory or your own Active Directory.	Can connect your own Active Directory and Azure Active Directory.
Network connection options include **No connectivity**.	Network connection options include only your own virtual networks.
When using Azure VNet peering to connect to your resources, you must create a VNet peer connection in Citrix DaaS for Azure.	Select an existing virtual network.
When importing an image from Azure, you specify the image's URI.	When importing an image, you can select a VHD or browse storage in the Azure subscription.
Can create a bastion machine in customer's Azure subscription to troubleshoot machines.	No need to create a bastion machine because you can already access the machines in your subscription.

View subscriptions

To view subscription details, from the **Manage > Azure Quick Deploy** dashboard in Citrix DaaS for Azure, expand **Cloud Subscriptions** on the right. Then click a subscription entry.

- The **Details** page includes the number of machines, plus the numbers and names of catalogs and images in the subscription.
- The **Resource Locations** page lists the resource locations where the subscription is used.

Add customer-managed Azure subscriptions

To use a customer-managed Azure subscription, you must add it to Citrix DaaS Standard for Azure before creating a catalog or image that uses that subscription. You have two options when adding your Azure subscriptions:

- **If you are a Global Administrator for the directory and have owner privileges for the subscription:** Simply authenticate to your Azure account.
- **If you are not a Global Administrator and have owner privileges on the subscription:** Before adding the subscription to Citrix DaaS for Azure, create an Azure app in your Azure AD and then add that app as a contributor of the subscription. When you add that subscription to Citrix DaaS for Azure, you provide relevant app information.

Add customer-managed Azure subscriptions if you're a Global Administrator

This task requires Global Administrator privileges for the directory, and owner privileges for the subscription.

1. From the **Manage > Azure Quick Deploy** dashboard in Citrix DaaS for Azure, expand **Cloud Subscriptions** on the right.
2. Click **Add Azure subscription**.
3. On the **Add Subscriptions** page, click **Add your Azure subscription**.
4. Select the button that allows Citrix DaaS for Azure to access your Azure subscriptions on your behalf.
5. Click **Authenticate Azure Account**. You're taken to the Azure sign-in page.
6. Enter your Azure credentials.
7. You're returned automatically to Citrix DaaS for Azure. The **Add Subscription** page lists the discovered Azure subscriptions. Use the search box to filter the list, if needed. Select one or more subscriptions. When you're done, click **Add Subscriptions**.
8. Confirm that you want to add the selected subscriptions.

The Azure subscriptions you selected are listed when you expand **Subscriptions**. Added subscriptions are available for selection when creating a catalog or image.

Add customer-managed Azure subscriptions if you're not a Global Administrator

Adding an Azure subscription when you're not a global admin is a two-part process:

- Before you add a subscription to Citrix DaaS for Azure, create an app in Azure AD and then add that app as a contributor of the subscription.
- Add the subscription to Citrix DaaS for Azure, using information about the app you created in Azure.

Create an app in Azure AD and add it as a contributor

1. Register a new application in Azure AD:

a) From a browser, navigate to https://portal.azure.com.

b) In the upper left menu, select **Azure Active Directory**.

c) In the **Manage** list, click **App registrations**.

d) Click **+ New registration**.

e) On the **Register an application** page, provide the following information:

- **Name:** Enter the connection name
- **Application type:** Select **Web app / API**
- **Redirect URI:** leave blank

f) Click **Create**.

2. Create the application's secret access key and add the role assignment:

a) From the previous procedure, select **App Registration** to view details.

b) Make a note of the **Application ID** and **Directory ID**. You'll use this later when adding your subscription to Citrix DaaS for Azure.

c) Under **Manage**, select **Certificates & secrets**.

d) On the **Client secrets** page, select **+ New client secret**.

e) On the **Add a client secret** page, provide a description and select an expiration interval. Then click **Add**.

f) Make a note of the client secret value. You'll use this later when adding your subscription to Citrix DaaS for Azure.

g) Select the Azure subscription you want to link (add) to Citrix DaaS for Azure, and then click **Access control (IAM)**.

h) In the **Add a role assignment** box, click **Add**.

i) On the **Add role assignment** tab, select the following:

- **Role:** Contributor
- **Assign access to:** Azure AD user, group, or service principal
- **Select:** The name of the Azure app you created earlier.

j) Click **Save**.

Add your subscription to Citrix DaaS for Azure You'll need the application ID, directory ID, and client secret value from the app you created in Azure AD.

1. From the **Manage > Azure Quick Deploy** dashboard in Citrix DaaS for Azure, expand **Cloud Subscriptions** on the right.

2. Click **Add Azure subscription**.
3. On the **Add Subscriptions** page, click **Add your Azure subscriptions**.
4. Select **I have an Azure App with contributor role to the subscription**.
5. Enter the tenant ID (directory ID), client ID (application ID), and client secret for the app you created in Azure.
6. Click **Select your subscription** and then select the subscription you want.

Later, from the subscription's **Details** page in the Citrix DaaS for Azure dashboard, you can update the client secret or replace the Azure app from the ellipsis menu.

If Citrix DaaS for Azure can't access an Azure subscription after it's added, several catalog power management and individual machine actions aren't allowed. A message provides an option to add the subscription again. If the subscription was originally added using an Azure app, you can replace the Azure app.

Add Citrix Managed Azure subscriptions

A Citrix Managed Azure subscription supports the number of machines indicated in Limits. (In this context, *machines* refers to VMs that have a Citrix VDA installed. These machines deliver apps and desktops to users. It does not include other machines in a resource location, such as Cloud Connectors.)

If your Citrix Managed Azure subscription is likely to reach its limit soon, and you have enough Citrix licenses, you can request another Citrix Managed Azure subscription. The dashboard contains a notification when you're close to the limit.

You can't create a catalog (or add machines to a catalog) if the total number of machines for all catalogs that use that Citrix Managed Azure subscription would exceed the value indicated in Limits.

For example, assume a hypothetical limit of 1,000 machines per Citrix Managed Azure subscription.

- Let's say you have two catalogs (`Cat1` and `Cat2`) that use the same Citrix Managed Azure subscription. `Cat1` currently contains 500 machines, and `Cat2` has 250.
- As you plan for future capacity needs, you add 200 machines to `Cat2`. The Citrix Managed Azure subscription now supports 950 machines (500 in `Cat 1` and 450 in `Cat 2`). The dashboard indicates that the subscription is near its limit.
- When you need 75 more machines, you can't use that subscription to create a catalog with 75 machines (or add 75 machines to an existing catalog). That would exceed the subscription limit. Instead, you request another Citrix Managed Azure subscription. Then, you can create a catalog using that subscription.

When you have more than one Citrix Managed Azure subscription:

- Nothing is shared between those subscriptions.
- Each subscription has a unique name.
- You can choose among the Citrix Managed Azure subscriptions (and any customer-managed Azure subscriptions that you've added) when:
  - Creating a catalog.
  - Building or importing an image.
  - Creating a VNet peering or SD-WAN connection.

Requirement:

- You must have enough Citrix licenses to warrant adding another Citrix Managed Azure subscription. Using the previous hypothetical example, if you have 2,000 Citrix licenses in anticipation of deploying at least 1,500 machines through Citrix Managed subscriptions, you can add another Citrix Managed Azure subscription.

To add a Citrix Managed Azure subscription:

1. Contact your Citrix representative to request another Citrix Managed Azure subscription. You are notified when you can proceed.
2. From the **Manage > Azure Quick Deploy** dashboard in Citrix DaaS for Azure, expand **Cloud Subscriptions** on the right.
3. Click **Add Azure subscription**.
4. On the **Add Subscriptions** page, click **Add a Citrix Managed Azure subscription**.
5. On the **Add a Citrix Managed Subscription** page, click **Add Subscription** at the bottom of the page.

If you're notified that an error occurred during creation of a Citrix Managed Azure subscription, contact Citrix Support.

Remove Azure subscriptions

To remove an Azure subscription, you must first delete all catalogs and images that use it.

If you have one or more Citrix Managed Azure subscriptions, you cannot remove all of them. At least one must remain.

1. From the **Manage > Azure Quick Deploy** dashboard in Citrix DaaS for Azure, expand **Cloud Subscriptions** on the right.
2. Click the subscription entry.
3. On the **Details** tab, click **Remove Subscription**.
4. Click **Authenticate Azure Account**. You're taken to the Azure sign-in page.
5. Enter your Azure credentials.

6. You're returned automatically to Citrix DaaS for Azure. Confirm the deletion in the check boxes and then click **Yes, Delete Subscription**.

Network connections

April 13, 2023

Introduction

This article provides details about several deployment scenarios when using a Citrix Managed Azure subscription.

When creating a catalog, you indicate if and how users access locations and resources on their corporate on-premises network from their Citrix DaaS Standard for Azure (formerly Citrix Virtual Apps and Desktops Standard for Azure) desktops and apps.

When using a Citrix Managed Azure subscription, the choices are:

- No connectivity
- Azure VNet peering
- SD-WAN

When using one of your own customer-managed Azure subscriptions, there is no need to create a connection to Citrix DaaS for Azure. You just add the Azure subscription to Citrix DaaS for Azure.

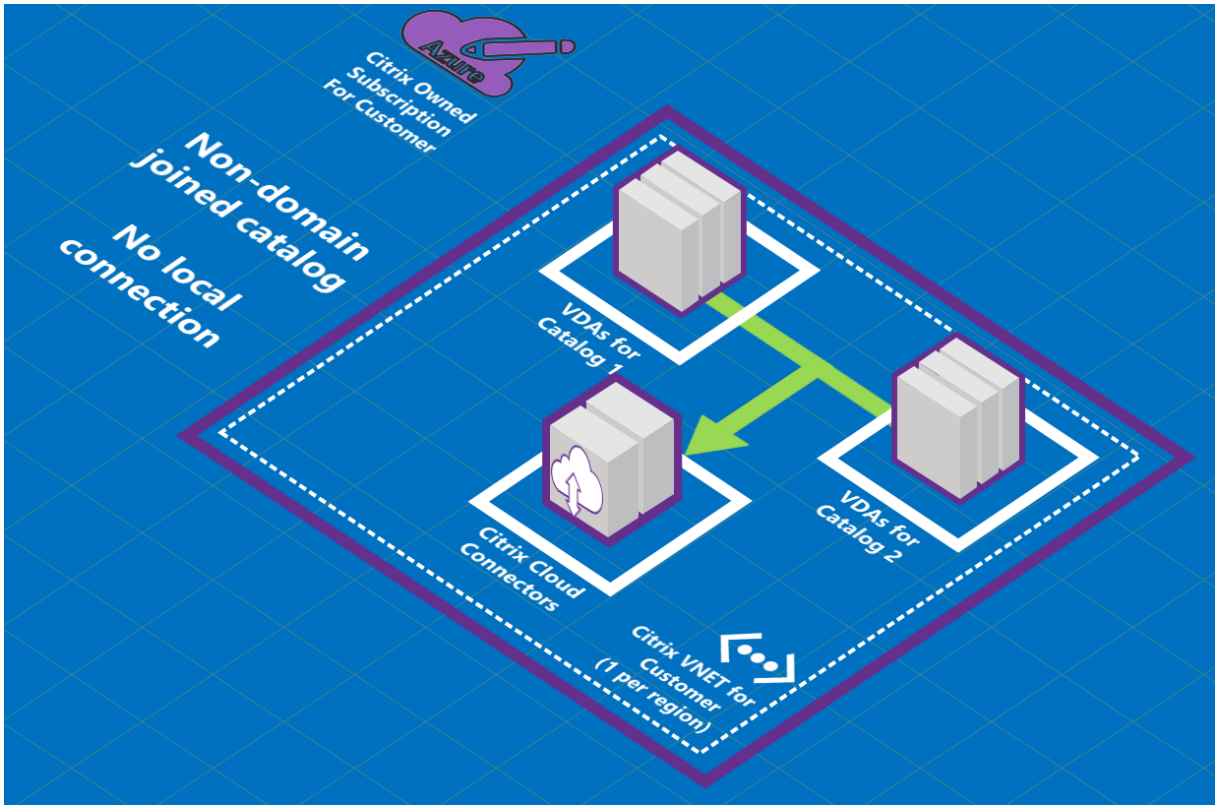
You cannot change a catalog's connection type after the catalog is created.

Requirements for all network connections

- When creating a connection, you must have valid DNS server entries.
- When using Secure DNS or a third-party DNS provider, you must add the address range that is allocated for use by Citrix DaaS for Azure to the DNS provider's IP addresses on the allow list. That address range is specified when you create a connection.
- All service resources that use the connection (domain-joined machines) must be able to reach your Network Time Protocol (NTP) server, to ensure time synchronization.

No connectivity

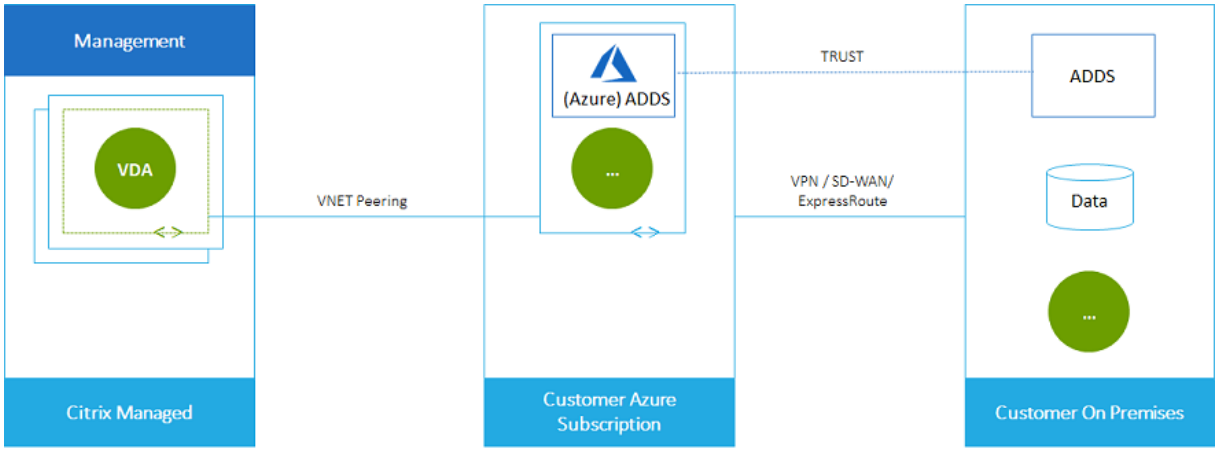
When a catalog is configured with **No connectivity**, users cannot access resources on their on-premises or other networks. This is the only choice when creating a catalog using quick create.



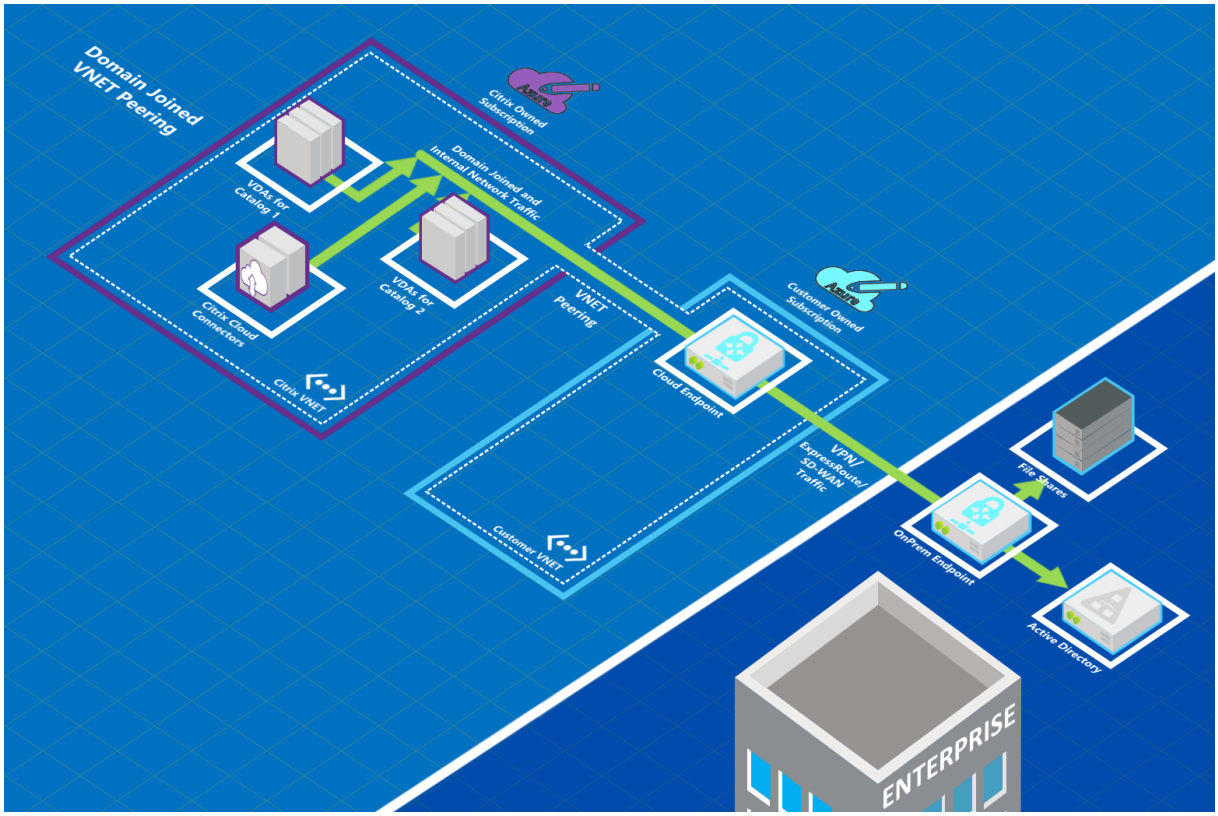
About Azure VNet peering connections

Virtual network peering seamlessly connects two Azure virtual networks (VNets): yours and the Citrix DaaS for Azure VNet. Peering also helps enable users to access files and other items from your on-premises networks.

As shown in the following graphic, you create a connection using Azure VNet peering from the Citrix Managed Azure subscription to the VNet in your company's Azure subscription.



Here's another illustration of VNet peering.



Users can access their on-premises network resources (such as file servers) by joining the local domain when you create a catalog. (That is, you join the AD domain where file shares and other needed resources reside.) Your Azure subscription connects to those resources (in the graphics, using a VPN or Azure ExpressRoute). When creating the catalog, you provide the domain, OU, and account credentials.

> **Important:**
>
> - Learn about VNet peering before using it in Citrix DaaS for Azure.
> - Create a VNet peering connection before creating a catalog that uses it.

Azure VNet peering custom routes

Custom, or user-defined, routes override Azure's default system routes for directing traffic between virtual machines in a VNet peering, on-premises networks, and the Internet. You might use custom routes if there are networks that Citrix DaaS for Azure resources are expected to access but aren't directly connected through VNet peering. For example, you might create a custom route that forces traffic through a network appliance to the Internet or to an on-premises network subnet.

To use custom routes:

- You must have an existing Azure virtual network gateway or a network appliance such as Citrix

SD-WAN in your Citrix DaaS for Azure environment.
- When you add custom routes, you must update your company's route tables with the Citrix DaaS for Azure destination VNet information to ensure end-to-end connectivity.
- Custom routes are displayed in Citrix DaaS for Azure in the order in which they are entered. This display order does not affect the order in which Azure selects routes.

Before using custom routes, review the Microsoft article Virtual network traffic routing to learn about using custom routes, next hop types, and how Azure selects routes for outbound traffic.

You can add custom routes when you create an Azure VNet peering connection or to existing ones in your Citrix DaaS for Azure environment. When you're ready to use custom routes with your VNet peering, refer to the following sections in this article:

- For custom routes with new Azure VNet peerings: Create an Azure VNet peering connection
- For custom routes with existing Azure VNet peerings: Manage custom routes for existing Azure VNet peer connections

Azure VNet peering requirements and preparation

- Credentials for an Azure Resource Manager subscription owner. This must be an Azure Active Directory account. Citrix DaaS for Azure does not support other account types, such as live.com or external Azure AD accounts (in a different tenant).
- An Azure subscription, resource group, and virtual network (VNet).
- Set up the Azure network routes so that VDAs in the Citrix Managed Azure subscription can communicate with your network locations.
- Open Azure network security groups from your VNet to the specified IP range.
- **Active Directory:** For domain-joined scenarios, we recommend that you have some form of Active Directory services running in the peered VNet. This takes advantage of the low latency characteristics of the Azure VNet peering technology.

  For example, the configuration might include Azure Active Directory Domain Services (AADDS), a domain controller VM in the VNet, or Azure AD Connect to your on-premises Active Directory.

  After you enable AADDS, you cannot move your managed domain to a different VNet without deleting the managed domain. So, it's important to select the correct VNet to enable your managed domain. Before proceeding, review the Microsoft article Networking considerations for Azure AD Domain Services.
- **VNet IP range:** When creating the connection, you must provide an available CIDR address space (IP address and network prefix) that is unique among the network resources and the Azure VNets being connected. This is the IP range assigned to the VMs within the Citrix DaaS for Azure peered VNet.

Ensure that you specify an IP range that does not overlap any addresses that you use in your Azure and on-premises networks.

- For example if your Azure VNet has an address space of 10.0.0.0 /16, create the VNet peering connection in Citrix DaaS for Azure as something such as 192.168.0.0 /24.
- In this example, creating a peering connection with a 10.0.0.0 /24 IP range would be considered an overlapping address range.

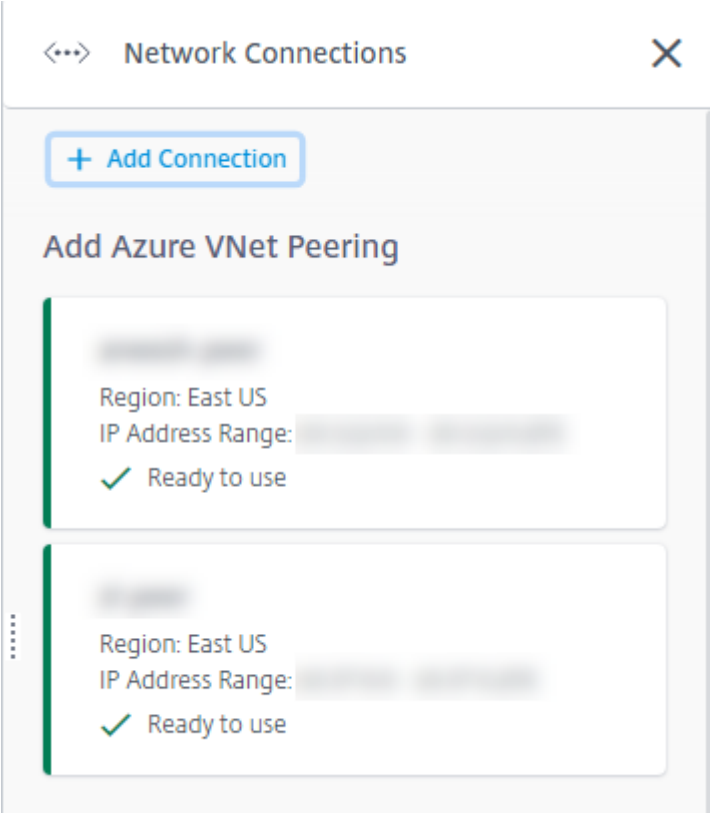
If addresses overlap, the VNet peering connection might not be created successfully. It also does not work correctly for site administration tasks.

To learn about VNet peering, see the following Microsoft articles.

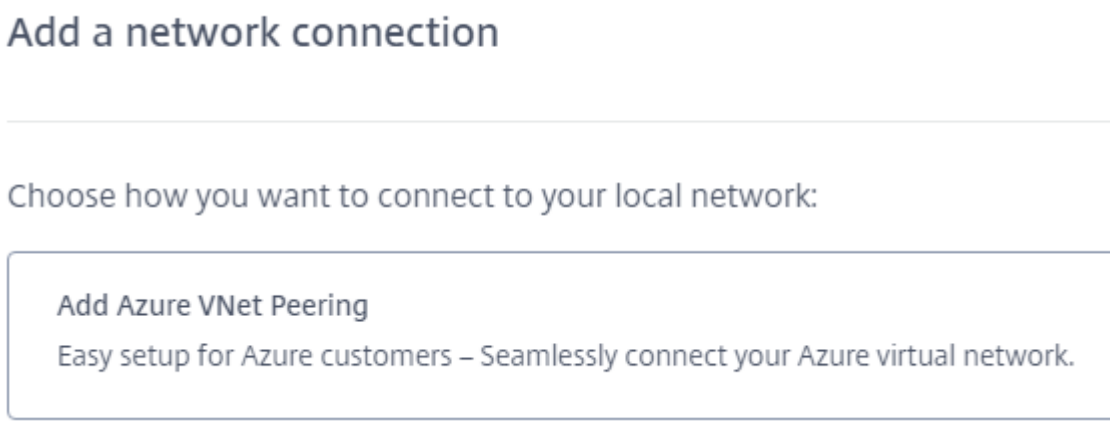
- Virtual network peering
- Azure VPN Gateway
- Create a Site-to-Site connection in the Azure portal
- VPN Gateway FAQ (search for "overlap")

Create an Azure VNet peering connection

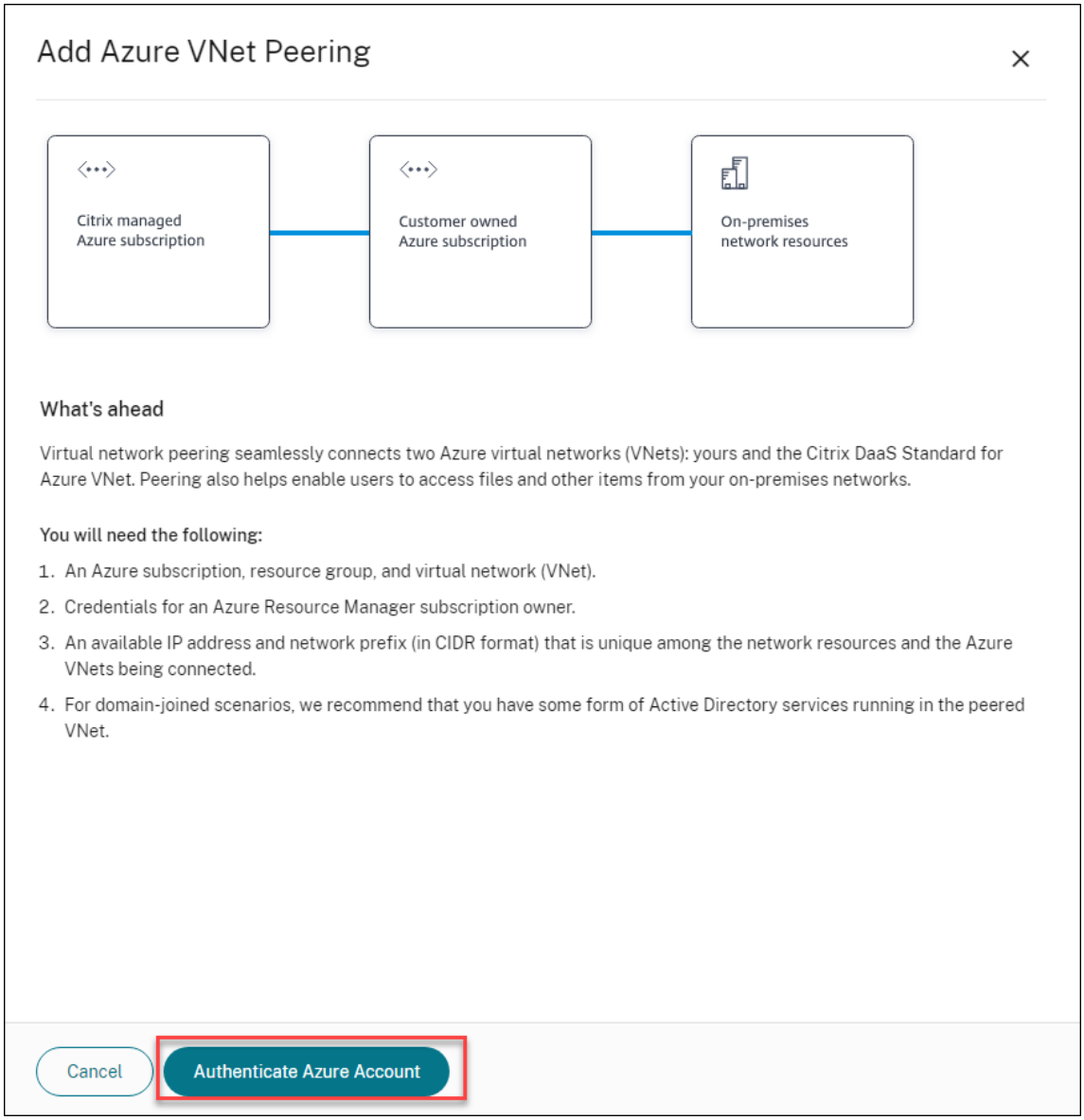
1. From the **Manage > Azure Quick Deploy** dashboard in Citrix DaaS for Azure, expand **Network Connections** on the right. If you have already set up connections, they're listed.



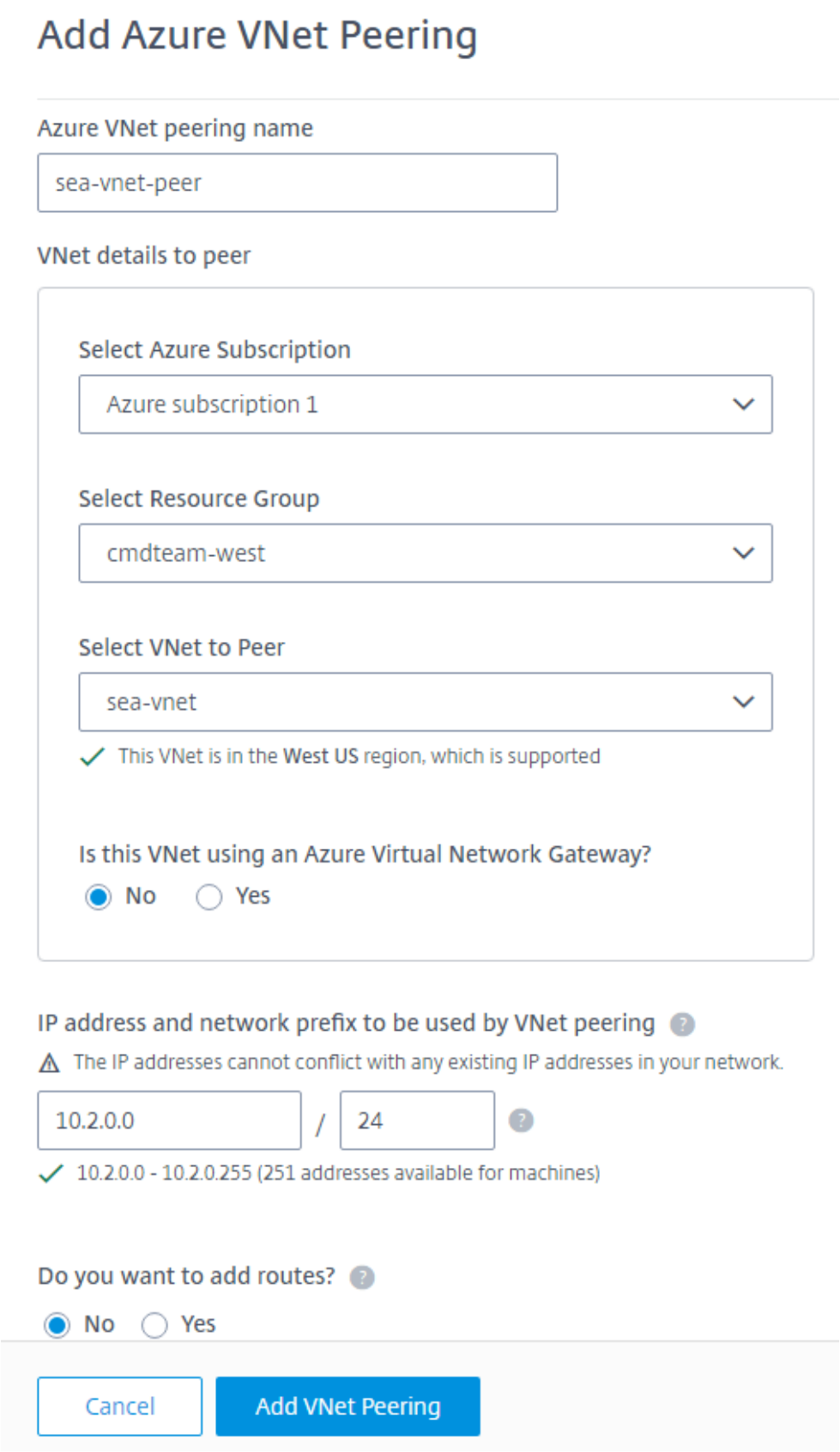
2. Click **Add Connection**.
3. Click anywhere in the **Add Azure VNet Peering** box.



4. Click **Authenticate Azure Account**.



5. Citrix DaaS for Azure automatically takes you to the Azure sign-in page to authenticate your Azure subscriptions. After you sign in to Azure (with the global administrator account credentials) and accept the terms, you are returned to the connection creation details dialog.



6. Type a name for the Azure VNet peer.
7. Select the Azure subscription, resource group, and the VNet to peer.
8. Indicate whether the selected VNet uses an Azure Virtual Network Gateway. For information, see the Microsoft article Azure VPN Gateway.
9. If you answered **Yes** in the previous step (the selected VNet uses an Azure virtual network gateway), indicate whether you want to enable virtual network gateway route propagation. When enabled, Azure automatically learns (adds) all routes through the gateway.

   You can change this setting later on the connection's **Details** page. However, changing it can cause route pattern changes and VDA traffic interruptions. Also, if you disable it later, you must manually add routes to networks that VDAs will use.
10. Type an IP address and select a network mask. The address range to be used is displayed, plus how many addresses that the range supports. Ensure that the IP range does not overlap any addresses that you use in your Azure and on-premises networks.

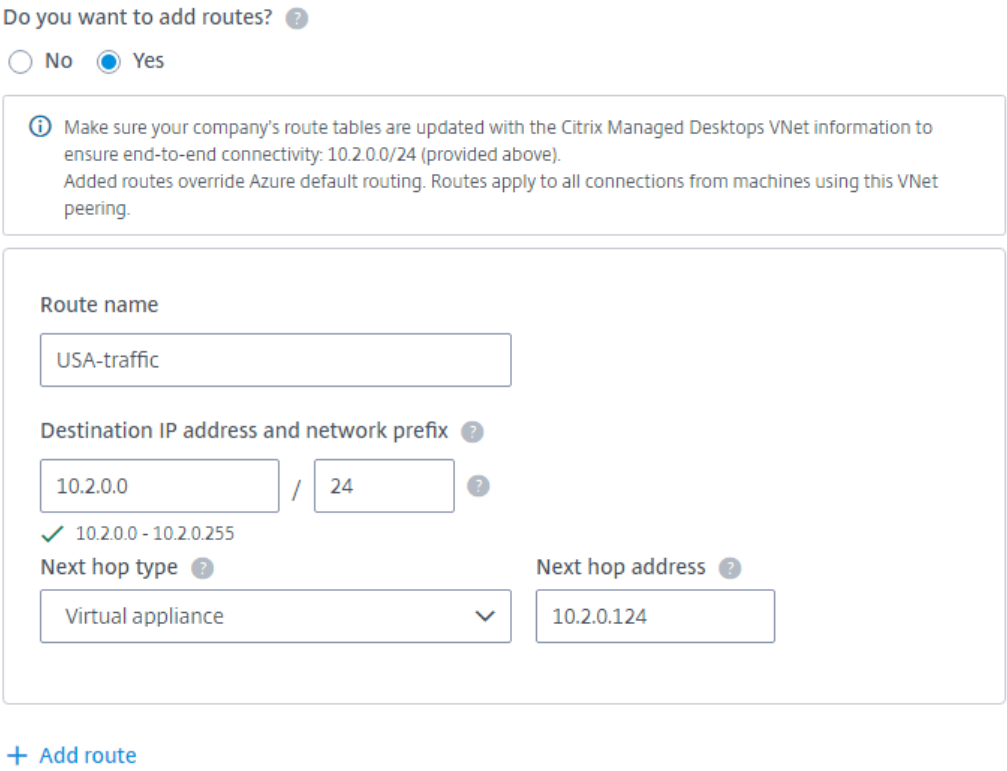
    - For example, if your Azure VNet has an address space of 10.0.0.0 /16, create the VNet peering connection in Citrix Virtual Apps and Desktops Standard as something such as 192.168.0.0 /24.
    - In this example, creating a VNet peering connection with a 10.0.0.0 /24 IP range would be considered an overlapping address range.

    If addresses overlap, the VNet peering connection might not be created successfully. It also won't work correctly for site administration tasks.
11. Indicate whether you want to add custom routes to the VNet peering connection. If you select **Yes**, enter the following information:

    a) Type a friendly name for the custom route.

    b) Enter the destination IP address and network prefix. The network prefix must be between 16 and 24.

    c) Select a next hop type for where you want traffic to be routed. If you select **Virtual appliance**, enter the internal IP address of the appliance.



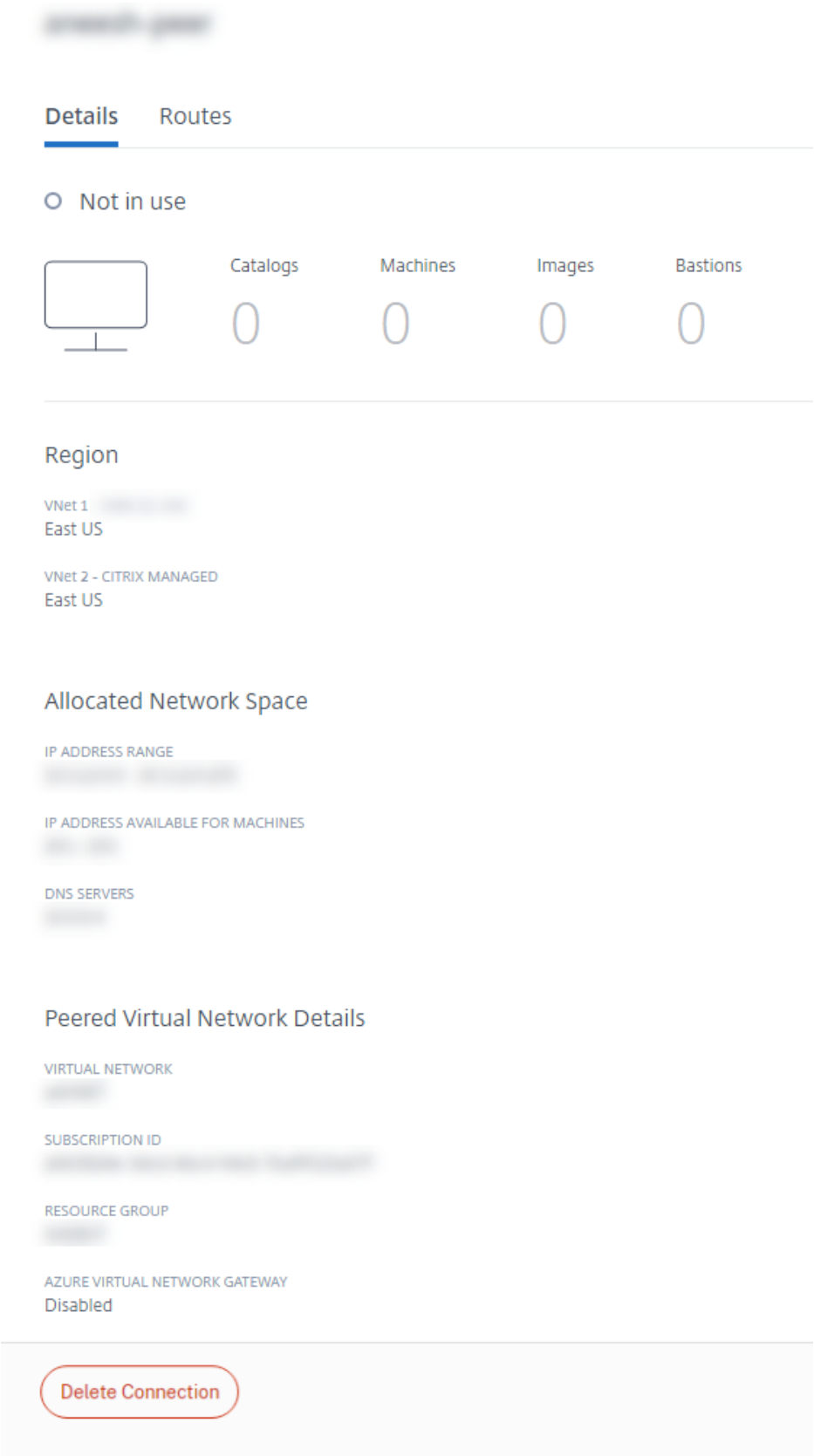
For more information about next hop types, see Custom routes in the Microsoft article Virtual network traffic routing.

d) Click **Add route** to create another custom route for the connection.

12. Click **Add VNet Peering**.

After the connection is created, it is listed under **Network Connections > Azure VNet Peers** on the right side of the **Manage > Azure Quick Deploy** dashboard. When you create a catalog, this connection is included in the available network connections list.

View Azure VNet peering connection details



1. From the **Manage > Azure Quick Deploy** dashboard in Citrix DaaS for Azure, expand **Network Connections** on the right.
2. Select the Azure VNet peering connection you want to display.

Details include:

- The number of catalogs, machines, images, and bastions that use this connection.
- The region, allocated network space, and peered VNets.
- The routes currently configured for the VNet peering connection.

Manage custom routes for existing Azure VNet peer connections

You can add new custom routes to an existing connection or modify existing custom routes, including disabling or deleting custom routes.

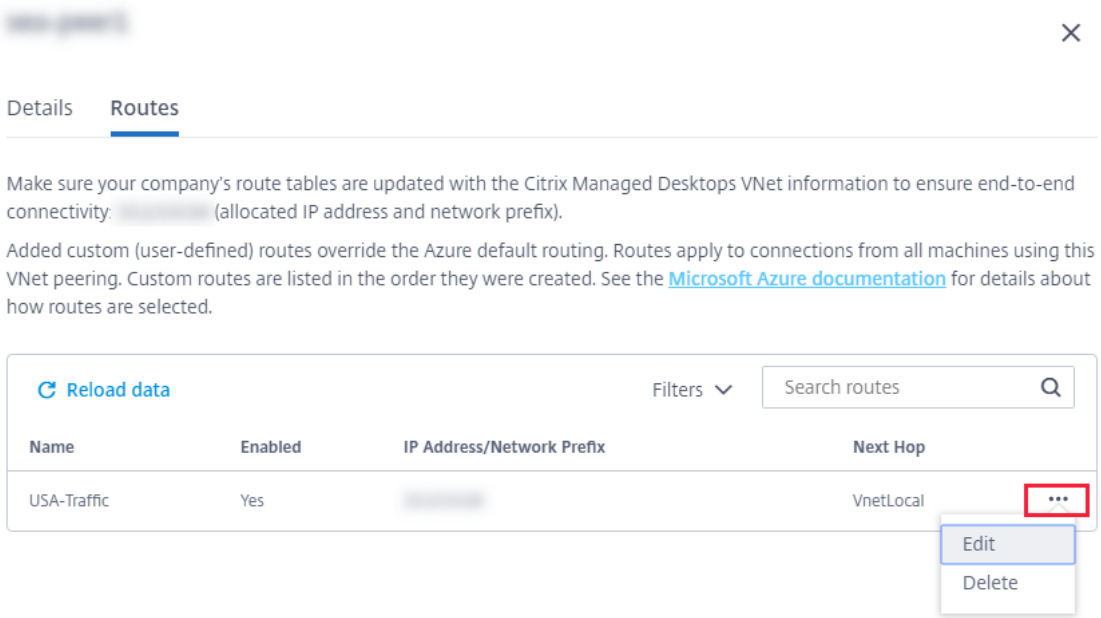
> **Important:**
>
> Modifying, disabling, or deleting custom routes changes the traffic flow of the connection and might disrupt any user sessions that might be active.

To add a custom route:

1. From the VNet peering connection details, select **Routes** and then click **Add Route**.
2. Enter a friendly name, the destination IP address and prefix, and the next hop type you want to use. If you select **Virtual Appliance** as the next hop type, enter the internal IP address of the appliance.
3. Indicate whether you want to enable the custom route. By default, the custom route is enabled.
4. Click **Add Route**.

To modify or disable a custom route:

1. From the VNet peering connection details, select **Routes** and then locate the custom route you want to manage.
2. From the ellipsis menu, select **Edit**.



3. Make any needed changes to the destination IP address and prefix or the next hop type, as needed.
4. To enable or disable a custom route, in **Enable this route?**, select **Yes** or **No**.
5. Click **Save**.

To delete a custom route:

1. From the VNet peering connection details, select **Routes** and then locate the custom route you want to manage.
2. From the ellipsis menu, select **Delete**.
3. Select **Deleting a route may disrupt active sessions** to acknowledge the impact of deleting the custom route.
4. Click **Delete Route**.

Delete an Azure VNet peering connection

Before you can delete an Azure VNet peer, remove any catalogs associated with it. See Delete a catalog.

1. From the **Manage > Azure Quick Deploy** dashboard in Citrix DaaS for Azure, expand **Network Connections** on the right.
2. Select the connection you want to delete.
3. From the connection details, click **Delete Connection**.

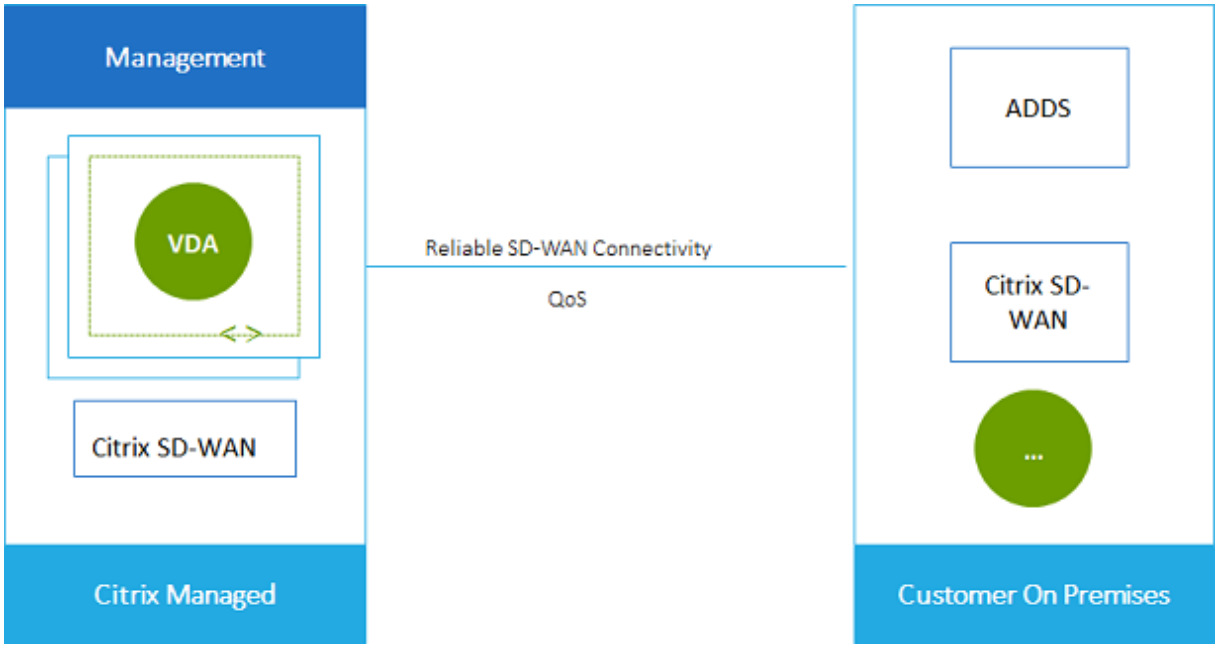
About SD-WAN connections

> **Important:**
>
> Citrix SD-WAN has been deprecated and all related content will be removed from the documentation in a future release. We recommend that you switch to alternative networking solutions to ensure uninterrupted access to Citrix services.

Citrix SD-WAN optimizes all the network connections needed by Citrix Virtual Apps and Desktops Standard for Azure. Working in concert with the HDX technologies, Citrix SD-WAN provides quality-of-service and connection reliability for ICA and out-of-band Citrix Virtual Apps and Desktops Standard traffic. Citrix SD-WAN supports the following network connections:

- Multi-stream ICA connection between users and their virtual desktops
- Internet access from the virtual desktop to websites, SaaS apps, and other cloud properties
- Access from the virtual desktop back to on-premises resources such as Active Directory, file servers, and database servers
- Real-time/interactive traffic carried over RTP from the media engine in the Workspace app to cloud-hosted Unified Communications services such as Microsoft Teams
- Client-side fetching of videos from sites like YouTube and Vimeo

As shown in the following graphic, you create an SD-WAN connection from the Citrix Managed Azure subscription to your sites. During connection creation, SD-WAN VPX appliances are created in the Citrix Managed Azure subscription. From the SD-WAN perspective, that location is treated as a branch.



SD-WAN connection requirements and preparation

- If the following requirements are not met, the SD-WAN network connection option is not available.
  - Citrix Cloud entitlements: Citrix Virtual Apps and Desktops Standard for Azure and SD-WAN Orchestrator.
  - An installed and configured SD-WAN deployment. The deployment must include a Master Control Node (MCN), whether in the cloud or on-premises, and be managed with SD-WAN Orchestrator.
- VNet IP range: Provide an available CIDR address space (IP address and network prefix) that is unique among the network resources being connected. This is the IP range assigned to the VMs within the Citrix Virtual Apps and Desktops Standard VNet.

  Ensure that you specify an IP range that does not overlap any addresses that you use in your cloud and on-premises networks.

  - For example, if your network has an address space of 10.0.0.0 /16, create the connection in Citrix Virtual Apps and Desktops Standard as something such as 192.168.0.0 /24.
  - In this example, creating a connection with a 10.0.0.0 /24 IP range would be considered an overlapping address range.

  If addresses overlap, the connection might not be created successfully. It also does not work correctly for site administration tasks.
- The connection configuration process includes tasks that you (the Citrix DaaS for Azure administrator) and the SD-WAN Orchestrator administrator must complete. Also, to complete your tasks, you need information provided by the SD-WAN Orchestrator administrator.

  We recommend that you both review the guidance in this document, plus the SD-WAN documentation, before actually creating a connection.

Create an SD-WAN connection

> **Important:**
>
> For details about SD-WAN configuration, see SD-WAN configuration for Citrix Virtual Apps and Desktops Standard for Azure integration.

1. From the **Manage > Azure Quick Deploy** dashboard in Citrix DaaS for Azure, expand **Network Connections** on the right.
2. Click **Add Connection**.
3. On the **Add a network connection** page, click anywhere in the SD-WAN box.

4. The next page summarizes what's ahead. When you're done reading, click **Start Configuring SD-WAN**.
5. On the **Configure SD-WAN** page, enter the information provided by your SD-WAN Orchestrator administrator.
   - **Deployment mode:** If you select **High availability**, two VPX appliances are created (recommended for production environments). If you select **Standalone**, one appliance is created. You cannot change this setting later. To change to the deployment mode, you'll have to delete and re-create the branch and all associated catalogs.
   - **Name:** Type a name for the SD-WAN site.
   - **Throughput and number of offices:** This information is provided by your SD-WAN Orchestrator administrator.
   - **Region:** The region where the VPX appliances will be created.
   - **VDA subnet and SD-WAN subnet:** This information is provided by your SD-WAN Orchestrator administrator. See SD-WAN connection requirements and preparation for information about avoiding conflicts.
6. When you're done, click **Create Branch**.
7. The next page summarizes what to look for on the **Manage > Azure Quick Deploy** dashboard. When you're done reading, click **Got it**.
8. On the **Manage > Azure Quick Deploy** dashboard, the new SD-WAN entry under **Network Connections** shows the progress of the configuration process. When the entry turns orange with the message **Awaiting activation by SD-WAN administrator**, notify your SD-WAN Orchestrator administrator.
9. For SD-WAN Orchestrator administrator tasks, see the SD-WAN Orchestrator product documentation.
10. When the SD-WAN Orchestrator administrator finishes, the SD-WAN entry under **Network Connections** turns green, with the message **You can create catalogs using this connection.**

View SD-WAN connection details

1. From the **Manage > Azure Quick Deploy** dashboard in Citrix DaaS for Azure, expand **Network Connections** on the right.
2. Select **SD-WAN** if it's not the only selection.
3. Click the connection you want to display.

The display includes:

- **Details tab:** Information you specified when configuring the connection.

- **Branch Connectivity tab:** Name, cloud connectivity, availability, bandwidth tier, role, and location for each branch and MCN.

Delete an SD-WAN connection

Before you can delete an SD-WAN connection, remove any catalogs associated with it. See Delete a catalog.

1. From the **Manage > Azure Quick Deploy** dashboard in Citrix DaaS for Azure, expand **Network Connections** on the right.
2. Select SD-WAN if it's not the only selection.
3. Click the connection you want to delete, to expand its details.
4. On the **Details** tab, click **Delete Connection**.
5. Confirm the deletion.

Azure VPN Technical Preview

The Azure VPN feature is available for technical preview.

About Azure VPN gateway connections

An Azure VPN gateway connection provides a communication link between your Citrix-managed Azure VDAs (desktops and apps) and your company's resources, such as on-premises networks or resources in other cloud locations. This is similar to setting up and connecting to a remote branch office.

The secure connectivity uses the industry-standard protocols Internet Protocol Security (IPsec) and Internet Key Exchange (IKE).

During the connection creation process:

- You provide information that Citrix uses to create the gateway and connection.
- Citrix creates a site-to-site route-based Azure VPN gateway. The VPN gateway forms a direct Internet Protocol Security (IPsec) tunnel between the Citrix-managed Azure subscription and your VPN's host device.
- After Citrix creates the Azure VPN gateway and connection, you update your VPN's configuration, firewall rules, and route tables. For this process, you use a public IP address that Citrix provides, and a pre-shared key (PSK) that you provided for creating the connection.

An example connection is illustrated in Create an Azure VPN gateway connection.

You do not need your own Azure subscription to create this type of connection.

You can also optionally use custom routes with this connection type.

Azure VPN gateway custom routes

Custom, or user-defined, routes override default system routes for directing traffic between virtual machines in your networks, and the Internet. You might use custom routes if there are networks that Citrix Virtual Apps and Desktops Standard resources are expected to access but aren't directly connected through an Azure VPN gateway. For example, you might create a custom route that forces traffic through a network appliance to the Internet or to an on-premises network subnet.

When you add custom routes to a connection, those routes apply to all machines that use that connection.

To use custom routes:

- You must have an existing virtual network gateway or a network appliance such as Citrix SD-WAN in your Citrix Virtual Apps and Desktops Standard environment.
- When you add custom routes, you must update your company's route tables with the destination VPN information to ensure end-to-end connectivity.
- Custom routes are displayed on the **Connection > Routes** tab in the order they are entered. This display order does not affect the order in which routes are selected.

Before using custom routes, review the Microsoft article Virtual network traffic routing to learn about using custom routes, next hop types, and how Azure selects routes for outbound traffic.

You can add custom routes when you create an Azure VPN gateway connection or to existing connections in your service environment.

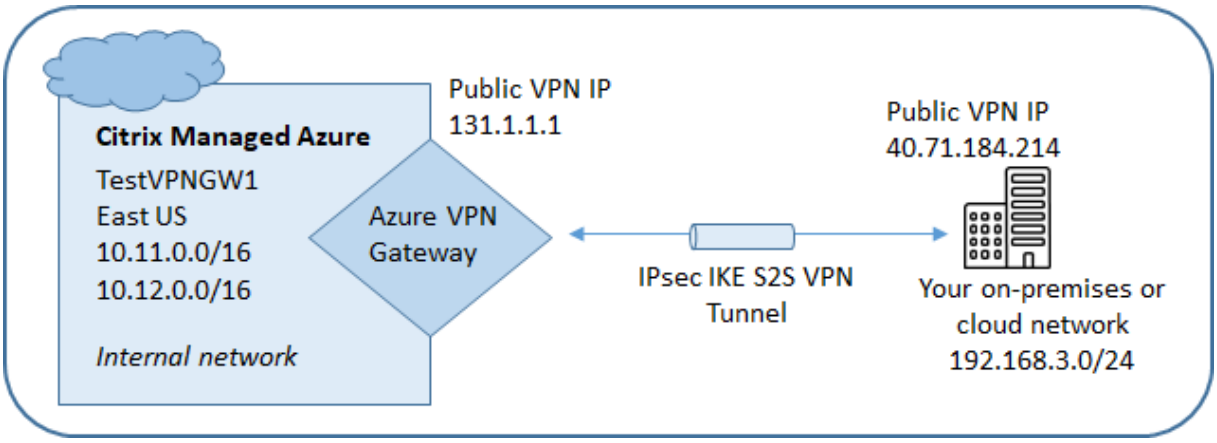
Azure VPN gateway connection requirements and preparation

- To learn about Azure VPN Gateway, see the Microsoft article What is VPN Gateway?
- Review the requirements for all network connections.
- You must have a configured VPN. The virtual network must be able to send and receive traffic through the VPN gateway. A virtual network can't be associated with more than one virtual network gateway.
- You must have an IPsec device that has a public IP address. To learn about validated VPN devices, see the Microsoft article About VPN devices.
- Review the Create an Azure VPN Gateway connection procedure before you actually start it, so you can collect the information you need. For example, you'll need allowed addresses in your network, IP ranges for the VDAs and gateway, desired throughput and performance level, and DNS server addresses.

Create an Azure VPN gateway connection

Be sure to review this procedure before actually starting it.

The following diagram shows an example of configuring an Azure VPN gateway connection. Generally, Citrix manages resources on the left side of the diagram, and you manage resources on the right side. Some descriptions in the following procedure include references to the diagram's examples.



1. From the **Manage** dashboard in Citrix DaaS for Azure, expand **Network Connections** on the right.
2. Click **Add Connection**.
3. Click anywhere in the **Azure VPN Gateway** box.
4. Review the information on the **Add VPN Connection** page, and then click **Start Configuring VPN**.
5. On the **Add a connection** page, provide the following information.
   - **Name:** A name for the connection. (In the diagram, the name is TestVPNGW1.)
   - **VPN IP address:** Your public-facing IP address.

     In the diagram, the address is 40.71.184.214.
   - **Allowed networks:** One or more address ranges that the Citrix service is allowed to access on your network. Usually, this address range contains the resources that your users need to access, such as file servers.

     To add more than one range, click **Add more IP addresses** and enter a value. Repeat as needed.

     In the diagram, the address range is 192.168.3.0/24.
   - **Pre-shared key:** A value that is used by both ends of the VPN for authentication (similar to a password). You decide what this value is. Be sure to note the value. You'll need it later when you configure your VPN with the connection information.

- **Performance and throughput:** The bandwidth level to use when your users access resources on your network.

  All choices do not necessarily support Border Gateway Protocol (BGP). In those cases, the **BCP settings** fields aren't available.

- **Region:** Azure region where Citrix deploys machines that deliver desktops and apps (VDAs), when you create catalogs that use this connection. You cannot change this selection after you create the connection. If you decide later to use a different region, you must create or use another connection that specifies the desired region.

  In the diagram, the region is EastUS.

- **Active-active (high availability) mode:** Whether two VPN gateways are created for high availability. When this mode is enabled, only one gateway is active at a time. Learn about active-active Azure VPN gateway in the Microsoft document Highly Available Cross-Premises Connectivity.

- **BGP settings:** (Available only if the selected **Performance and throughput** supports BGP.) Whether to use Border Gateway Protocol (BGP). Learn about BGP in the Microsoft document: About BGP with Azure VPN Gateway. If you enable BGP, provide the following information:

  - **Autonomous system number (ASN):** Azure virtual network gateways are assigned a default ASN of 65515. A BGP-enabled connection between two network gateways requires that their ASNs be different. If needed, you can change the ASN now or after the gateway is created.

  - **BGP IP peering IP address:** Azure supports BGP IP in the range 169.254.21.*x* to 169.254.22.*x*.

- **VDA subnet:** The address range where Citrix VDAs (machines that deliver desktops and apps) and Cloud Connectors will reside when you create a catalog that uses this connection. After you enter an IP address and select a network mask, the address range is displayed, plus how many addresses that the range supports.

  Although this address range is maintained in the Citrix-managed Azure subscription, it functions as if it is an extension of your network.

  - The IP range must not overlap any addresses that you use in your on-premises or other cloud networks. If addresses overlap, the connection might not be created successfully. Also, an overlapping address won't work correctly for site administration tasks.

  - The VDA subnet range must be different from the gateway subnet address.

  - You cannot change this value after you create the connection. To use a different value, create another connection.

In the diagram, the VDA subnet is 10.11.0.0/16.

- **Gateway subnet:** The address range where the Azure VPN gateway will reside when you create a catalog that uses this connection.
  - The IP range must not overlap any addresses that you use in your on-premises or other cloud networks. If addresses overlap, the connection might not be created successfully. Also, an overlapping address won't work correctly for site administration tasks.
  - The gateway subnet range must be different from the VDA subnet address.
  - You cannot change this value after you create the connection. To use a different value, create another connection.

  In the diagram, the gateway subnet is 10.12.0.9/16.

- **Routes:** Indicate whether you want to add custom routes to the connection. If you want to add custom routes, provide the following information:
  - Type a friendly name for the custom route.
  - Enter the destination IP address and network prefix. The network prefix must be between 16 and 24.
  - Select a next hop type for where you want traffic to be routed. If you select **Virtual appliance, enter the internal IP address of the appliance. For more information about next hop types, see Custom routes in the Microsoft article Virtual network traffic routing.

To add more than one route, click **Add route** and enter the requested information.

- **DNS servers:** Enter addresses for your DNS servers, and indicate the preferred server. Although you can change the DNS server entries later, keep in mind that changing them can potentially cause connectivity issues for the machines in catalogs that use this connection.

  To add more than two DNS server addresses, click **Add alternate DNS** and then enter the requested information.

6. Click **Create VPN Connection**.

After Citrix creates the connection, it is listed under **Network Connections > Azure VPN Gateway** on the **Manage** dashboard in Citrix DaaS for Azure. The connection card contains a public IP address. (In the diagram, the address is 131.1.1.1.)

- Use this address (and the pre-shared key you specified when creating the connection) to configure your VPN and firewalls. If you forgot your pre-shared key, you can change it on the connection's **Details** page. You'll need the new key to configure your end of the VPN gateway.

  For example, allow exceptions in your firewall for the VDA and gateway subnet IP address ranges you configured.

- Update your company's route tables with the Azure VPN gateway connection information to ensure end-to-end connectivity.

  In the diagram, new routes are required for traffic going from 192.168.3.0/24 to 10.11.0.0/16 and 10.12.0.9/16 (the VDA and gateway subnets).

- If you configured custom routes, make the appropriate updates for them, too.

When both ends of the connection are successfully configured, the connection's entry in **Network Connections > Azure VPN Gateway** indicates **Ready to use**.

View an Azure VPN gateway connection

1. From the **Manage** dashboard in Citrix DaaS for Azure, expand **Network Connections** on the right.
2. Select the connection you want to display.

   Displays:

- The **Details** tab shows the number of catalogs, machines, images, and bastions that use this connection. It also contains most of the information you configured for this connection.
- The **Routes** tab lists custom route information for the connection.

Manage custom routes for an Azure VPN gateway connection

In an existing Azure VPN gateway connection, you can add, modify, disable, and delete custom routes.

For information about adding custom routes when you create a connection, see Create an Azure VPN gateway connection.

> **Important:**
>
> Modifying, disabling, or deleting custom routes changes the traffic flow of the connection, and might disrupt active user sessions.

1. From the **Manage** dashboard in Citrix DaaS for Azure, expand **Network Connections** on the right.
2. Select the connection you want to display.

   - To add a custom route:

     a) From the connection's **Routes** tab, click **Add Route**.

b) Enter a friendly name, the destination IP address and prefix, and the next hop type you want to use. If you select **Virtual Appliance** as the next hop type, enter the internal IP address of the appliance.

c) Indicate whether you want to enable the custom route. By default, the custom route is enabled.

d) Click **Add Route**.

- To modify or enable/disable a custom route:

  a) From the connection's **Routes** tab, locate the custom route you want to manage.

  b) From the ellipsis menu, select **Edit**.

  c) Change the destination IP address and prefix, or the next hop type, as needed.

  d) Indicate whether you want to enable the route.

  e) Click **Save**.

- To delete a custom route:

  a) From the connection's **Routes** tab, locate the custom route you want to manage.

  b) From the ellipsis menu, select **Delete**.

  c) Select **Deleting a route may disrupt active sessions** to acknowledge the impact of deleting the custom route.

  d) Click **Delete Route**.

Reset or delete an Azure VPN gateway connection

> **Important:**
>
> - Resetting a connection causes the current connection to be lost, and both ends must reestablish it. A reset disrupts active user sessions.
> - Before you can delete a connection, delete any catalogs that use it. See Delete a catalog.

To reset or delete a connection:

1. From the **Manage** dashboard in Citrix DaaS for Azure, expand **Network Connections** on the right.
2. Select the connection you want to reset or delete.
3. From the connection's **Details** tab:

   - To reset the connection, click **Reset Connection**.

- To delete the connection, click **Delete Connection**.

4. If prompted, confirm the action.

Create a public static IP address

If you want all machines VDAs on a connection to use a single outbound public static IP address (gateway) to the Internet, enable a NAT gateway. You can enable a NAT gateway for connections to catalogs that are domain joined or non-domain joined.

To enable a NAT gateway for a connection:

1. From the **Manage > Azure Quick Deploy** dashboard in Citrix DaaS for Azure, expand **Network Connections** on the right.
2. Under **Network Connections**, select a connection under **CITRIX MANAGED** or **AZURE VNET PEERINGS**.
3. In the connection details card, click **Enable NAT Gateway**.
4. In the Enable NAT Gateway page, move the slider to **Yes** and configure an idle time.
5. Click **Confirm Changes**.

When you enable a NAT gateway:

- Azure assigns a public static IP address to the gateway automatically. (You cannot specify this address.) All VDAs in all catalogs that use this connection will use that address for outbound connectivity.
- You can specify an idle timeout value. That value indicates the number of minutes that an open outbound connection through the NAT gateway can remain idle before the connection is closed.
- You must allow the public static IP address in your firewall.

You can go back to the connection details card to enable or disable the NAT gateway and change the timeout value.

Images

April 12, 2024

When you create a catalog to deliver desktops or apps, an image is used (with other settings) as a template for creating the machines.

Citrix prepared images

Citrix DaaS Standard for Azure (formerly Citrix Virtual Apps and Desktops Standard for Azure) provides several Citrix prepared images:

- Windows 11 Pro (single-session)
- Windows 11 Enterprise Virtual Desktop (multi-session)
- Windows 11 Enterprise Virtual Desktop (multi-session) with Office 365 ProPlus
- Windows 10 Pro (single-session)
- Windows 10 Enterprise Virtual Desktop (multi-session)
- Windows 10 Enterprise Virtual Desktop (multi-session) with Office 365 ProPlus
- Windows Server 2022 (multi-session)
- Windows Server 2019 (multi-session)
- Windows Server 2016 (multi-session)
- Linux Ubuntu 22.04 LTS (single-session)
- Linux Ubuntu 22.04 LTS (multi-session)

The Citrix prepared images have a current Citrix Virtual Delivery Agent (VDA) and troubleshooting tools installed. The VDA is the communication mechanism between your users' machines and the Citrix Cloud infrastructure that manages Citrix DaaS for Azure. Images provided by Citrix are notated as **CITRIX**.

You can also import and use your own image from Azure.

Ways to use images

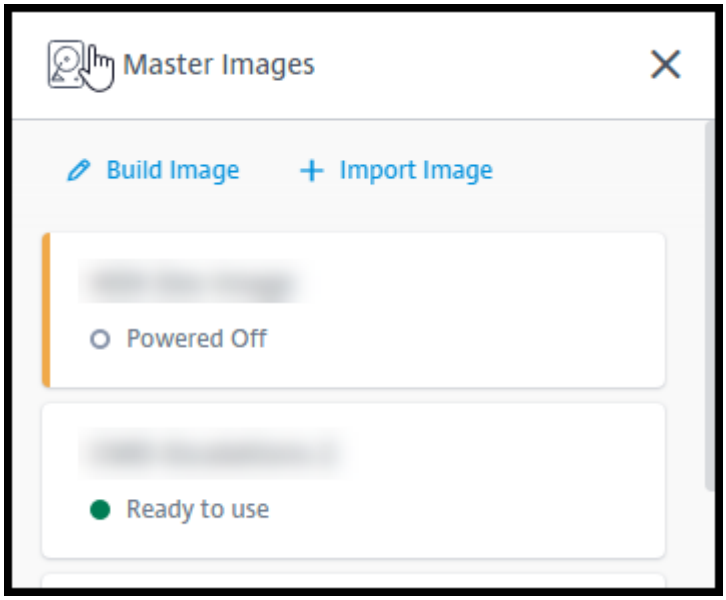
You can:

- **Use a Citrix prepared image when creating a catalog.** This choice is recommended only for proof of concept deployments.
- **Use a Citrix prepared image to create another image.** After the new image created, you customize it by adding applications and other software that your users need. Then, you can use that customized image when creating a catalog.
- **Import an image from Azure.** After you import an image from Azure, you can then use that image when creating a catalog. Or, you can use that image to create a new image, and then customize it by adding apps. Then, you can use that customized image when creating a catalog.

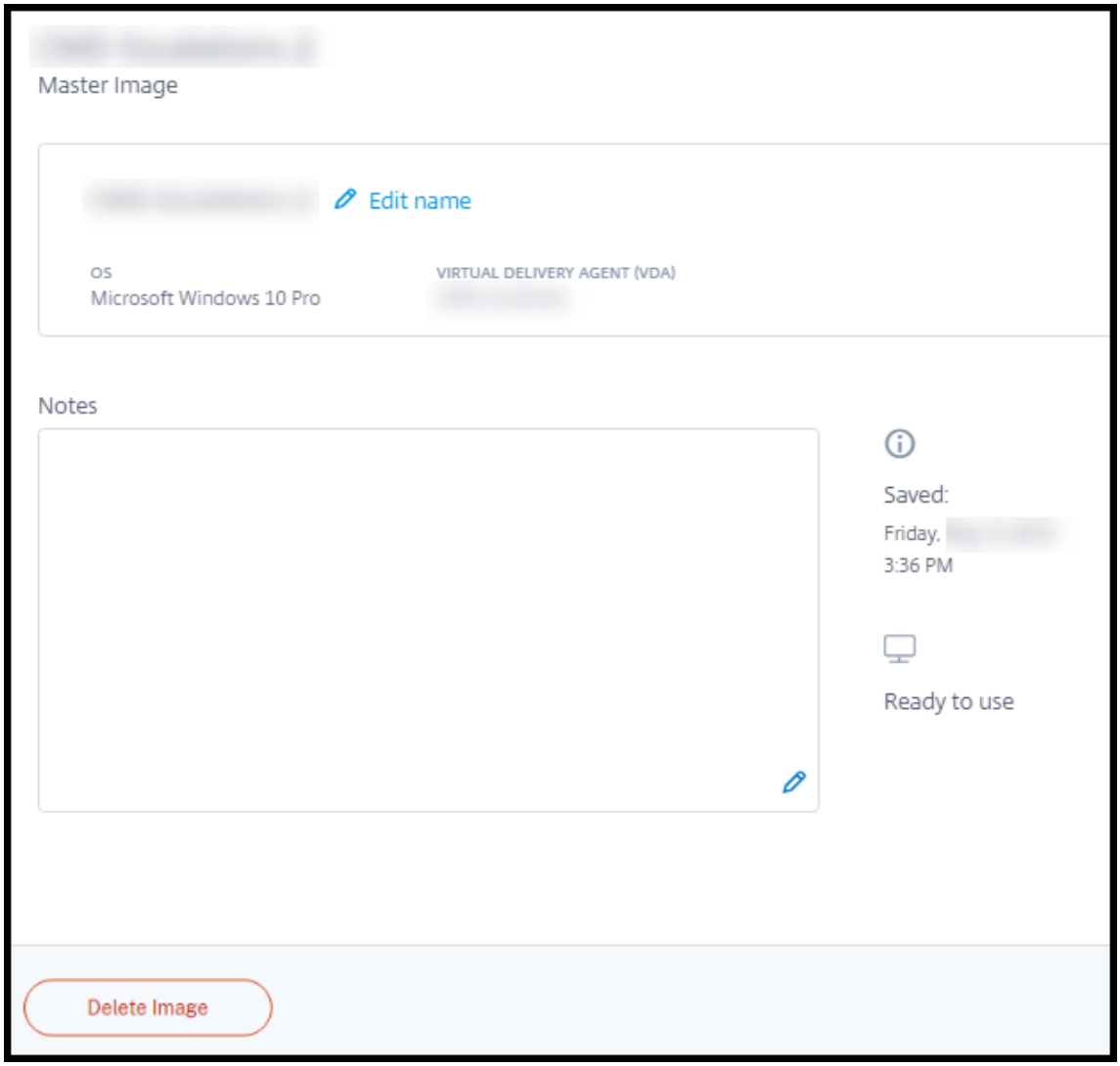
When you create a catalog, Citrix DaaS for Azure verifies that the image uses a valid operating system, and has a Citrix VDA and troubleshooting tools installed (along with other checks).

Display image information

1. From the **Manage > Azure Quick Deploy** dashboard, expand **Master Images** on the right. The display lists the images that Citrix provides, and images you created and imported.



2. Click an image to display its details.



From the details card, you can:

- Change (edit) the image's name.
- Add and edit notes (Available only for images you prepared or imported, not Citrix-provided images).
- Delete the image.

Prepare a new image

Preparing a new image includes creating the image and then customizing it. When you create an image, a new VM is created to load the new image.

Requirements:

- Know the performance characteristics that the machines need. For example, running CAD apps might require different CPU, RAM, and storage than other office apps.

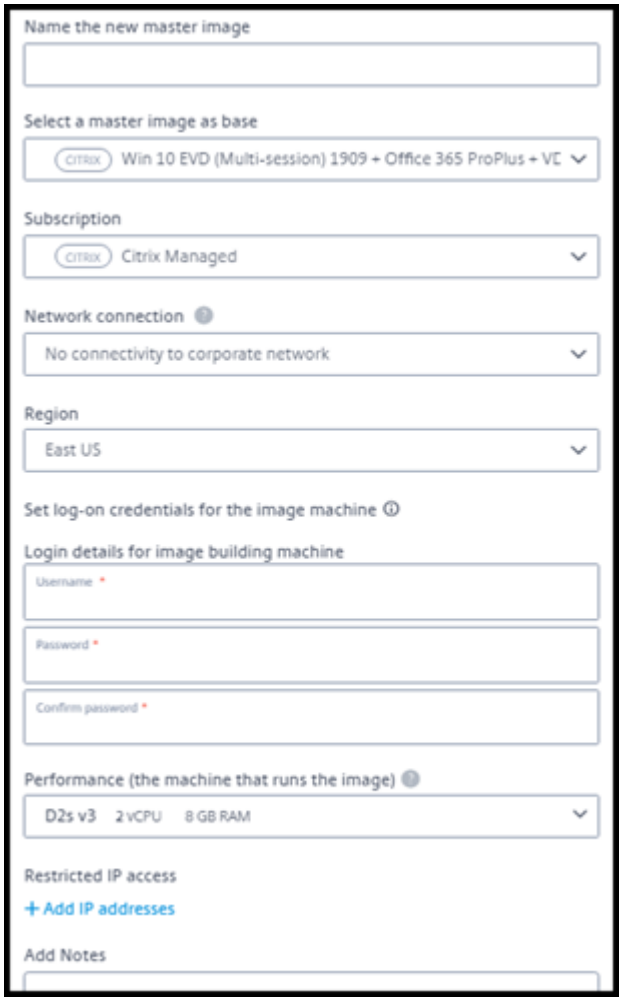
- If you plan to use a connection to your on-premises resources, set up that connection before creating the image and the catalog. For details, see Network connections.

When using a Citrix prepared Ubuntu image to build a new image, a root password is created for the new image. You can change that root password, but only during the image creation and customization process. (You cannot change the root password after the image is used in a catalog.)

- When the image is created, the administrator account that you specified (**Login details for image building machine**) is added to the `sudoers` group.
- After you RDP to the machine containing the new image, launch the terminal application and type `sudo passwd root`. When prompted, provide the password you specified when creating the image. After verification, you're prompted to enter a new password for the root user.

To create an image:

1. From the **Manage > Azure Quick Deploy** dashboard, expand **Master Images** on the right.
2. Click **Build Image**.



3. Enter values in the following fields:

- **Name:** Enter a name for the new image.
- **Master image:** Select an existing image. This is the base image that is used to create the new image.
- **Subscription:** Select an Azure subscription. For details, see Azure subscriptions.
- **Network connection:**
  - If using a Citrix Managed Azure subscription, select **No connectivity** or a previously created connection.
  - If using your own customer-managed Azure subscription, select your resource group, virtual network, and subnet. Then add domain details: FQDN, OU, service account name, and credentials.
- **Domain configuration:** Select the domain type: Active Directory or non-domain-joined.
  - If you select Active Directory, select or add a domain. Specify an OU (optional), service account name, and password.
  - If you select non-domain-joined, no additional information is needed.
- **Region:** (Available only for **No connectivity**.) Select a region where you want the machine containing the image to be created.
- **Logon credentials for image machine:** You'll use these credentials later when you connect (RDP) to the machine containing the new image, so that you can install apps and other software.
- **Machine performance:** This is CPU, RAM, and storage information for the machine that runs the image. Select a machine performance that meets your apps' requirements.
- **Restricted IP access:** If you want to restrict access to specific addresses, select **Add IP addresses** and then enter one or more addresses. After adding the addresses, click **Done** to return to the **Build image** card.
- **Notes:** Optionally add up to 1024 characters of notes. After the image is created, you can update the notes from the image's details display.
- **Local domain join:** Indicate whether you want to join the local Active Directory domain.
  - If you select **Yes**, enter the Azure information: FQDN, OU, service account name, and credentials.
  - If you select **No**, enter the credentials for the host machine.

4. When you're done, click **Build Image**.

An image can take up to 30 minutes to build. On the **Manage > Azure Quick Deploy** dashboard, expand **Master Images** on the right to see the current state (such as **Building image** or **Ready to customize**).

What to do next: Connect to a new image and customize it.

Connect to a new image and customize it

After a new image is created, its name is added to the images list, with a status of **Ready to customize** (or similar wording). To customize that image, you first download an RDP file. When you use that file to connect to the image, you can then add applications and other software to the image.

1. From the **Manage > Azure Quick Deploy** dashboard, expand **Master Images** on the right. Click the image you want to connect to.
2. Click **Download RDP file**. An RDP client downloads.

   The image machine might power off if you do not RDP to it shortly after it's created. This saves costs. When that happens, click **Power On**.
3. Double-click the downloaded RDP client. It automatically attempts to connect to the address of the machine containing the new image. When prompted, enter the credentials you specified when creating the image.
4. After you connect to the machine, add or remove apps, install updates, and finish any other customization work.

   Do **NOT** Sysprep the image.
5. When you're done customizing the new image, return to the **Master Images** box and click **Finish build**. The new image automatically undergoes validation testing.

Later, when you create a catalog, the new image is included in the list of images you can select.

On the **Manage > Quick Deploy** dashboard, the images display on the right indicates how many catalogs and machines use each image.

> **Note:**
>
> After you finalize an image, you cannot edit it. You must create a new image (using the previous image as a starting point), and then update the new image.

Import an image from Azure

When you import an image from Azure that has a Citrix VDA and applications your users need, you can use it to create a catalog or replace the image in an existing catalog.

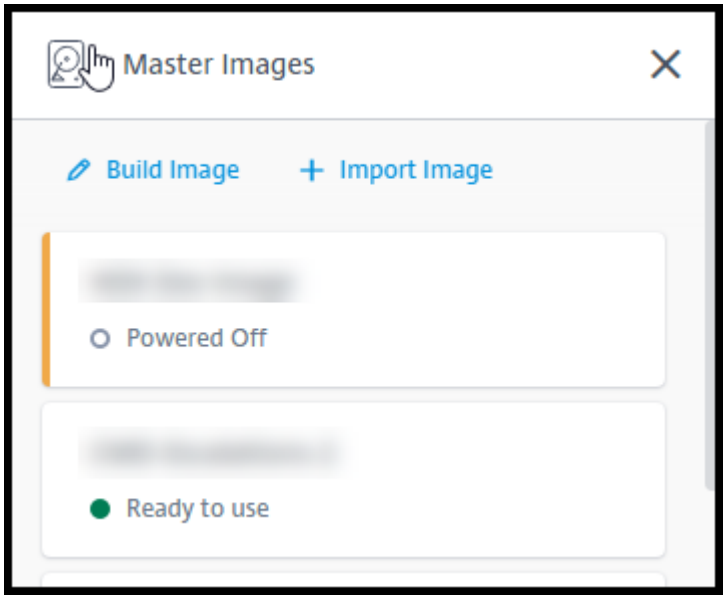
Imported image requirements

Citrix runs validation tests on the imported image. Ensure that the following requirements are met when you prepare the image that you'll import into Citrix DaaS for Azure.

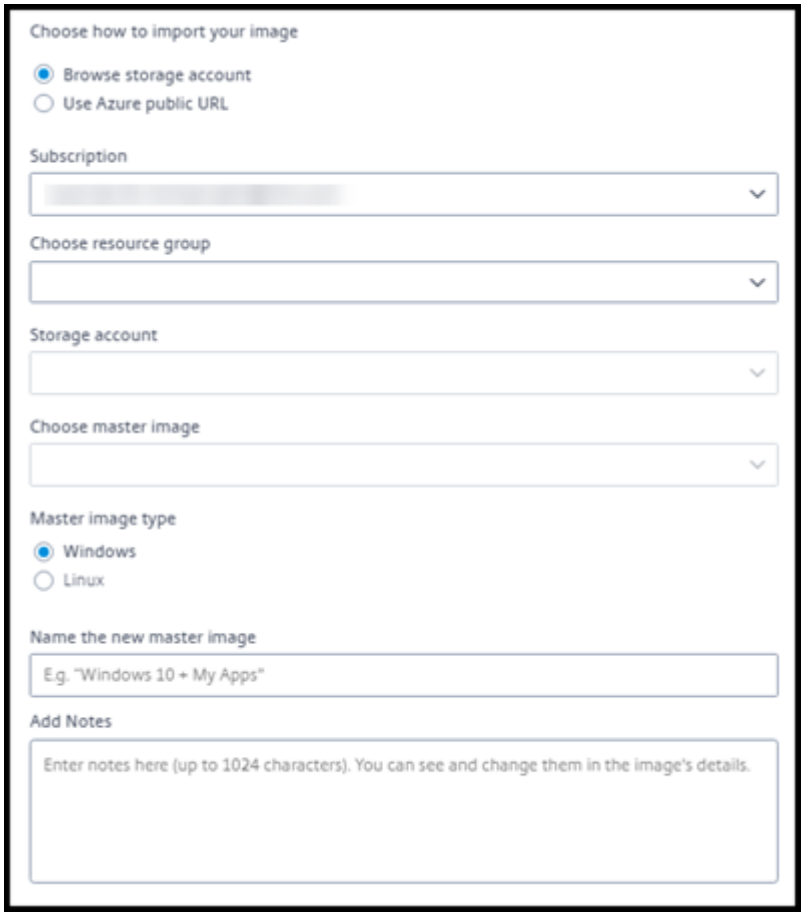
- **Supported OS:** The image must be a supported OS. To check a Windows OS version, run `Get-WmiObject Win32_OperatingSystem`.
- **Supported generation:** Generation 1 virtual machines support most guest operating systems. Generation 2 virtual machines support most 64-bit versions of Windows and more current version of Linux operating systems.
- **Not generalized:** The image must not be generalized.
- **No configured Delivery Controllers:** Ensure that no Citrix Delivery Controllers are configured in the image. Ensure that the following registry keys are cleared.
  - `HKLM:\SOFTWARE\Citrix\VirtualDesktopAgent\ListOfDDCs`
  - `HKLM:\SOFTWARE\Policies\Citrix\VirtualDesktopAgent\ListOfDDCs`
  - `HKLM:\SOFTWARE\Citrix\VirtualDesktopAgent\FarmGUID`
  - `HKLM:\SOFTWARE\Policies\Citrix\VirtualDesktopAgent\FarmGUID`
- **Personality.ini file:** The `personality.ini` file must exist on the system drive.
- **Valid VDA:** The image must have a Citrix VDA newer than 7.11 installed.
  - Windows: To check, use `Get HKLM:\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\Citrix Virtual Desktop Agent`. For installation guidance, see Install a Windows VDA on an image.
  - Red Hat Enterprise Linux and Ubuntu: For installation guidance, see the product documentation.
- **Azure Virtual Machine Agent:** Before importing an image, make sure that the Azure Virtual Machine Agent is installed on the image. For more information, see the Microsoft article Azure Virtual Machine Agent overview.

Import the image

1. From the **Manage > Azure Quick Deploy** dashboard, expand **Master Images** on the right.



2. Click **Import Image**.



3. Choose how to import the image.

   - For managed disks, use the export feature to generate a SAS URL. Set the expiration time

to 7200 seconds or more.
- For VHDs in a storage account, choose one of the following:
  - Generate a SAS URL for the VHD file.
  - Update the access level of a block storage container to blob or container. Then, get the file's URL.

4. If you selected **Browse storage account**:
   a) Sequentially select a subscription > resource group > storage account > image.
   b) Name the image.
5. If you selected **Azure public URL**:
   a) Enter the Azure-generated URL for the VHD. For guidance, click the link to the Microsoft document Download a Windows VHD from Azure.
   b) Select a subscription. (A Linux image can be imported only if you select a customer-managed subscription.)
   c) Name the image.
6. When you're done, click **Import Image**.

Update a catalog with a new image

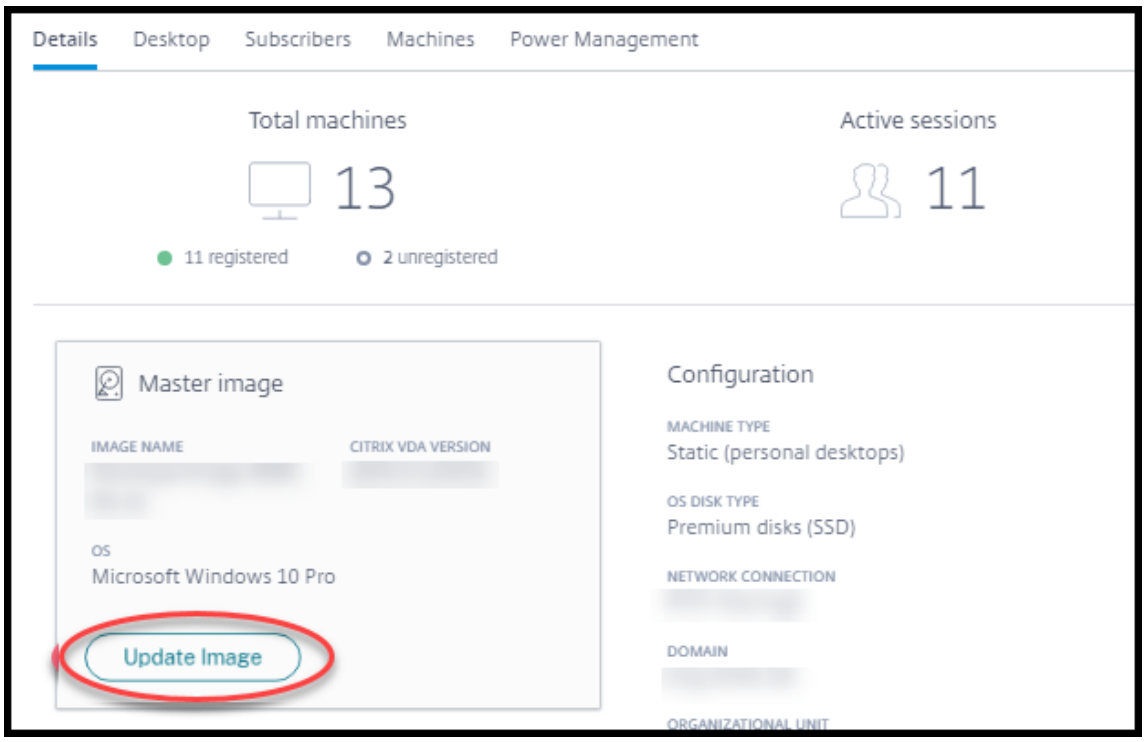
The catalog type determines which machines are updated when you update the catalog.

- For a random catalog, all the machines currently in the catalog are updated with the latest image. If you add more desktops to that catalog, they are based on the latest image.
- For a static catalog, the machines currently in the catalog are not updated with the latest image. Machines currently in the catalog continue to use the image they were created from. However, if you add more machines to that catalog, they are based on the latest image.

You can update a catalog containing machines with gen1 images with a gen2 image, if the catalog's machines support gen2. Similarly, you can update a catalog containing gen2 machines with a gen1 image, if the catalog's machines support gen1.

To update a catalog with a new image:

1. From the **Manage > Azure Quick Deploy** dashboard, click anywhere in the catalog's entry.
2. On the **Details** tab, click **Update Image**.



3. Select an image.
4. For random or multi-session catalogs: Select a logoff interval. After Citrix DaaS for Azure completes the initial image processing, subscribers receive a warning to save their work and log off from their desktops. The logoff interval indicates how long subscribers have after receiving the message until the session ends automatically.
5. Click **Update Image**.

Delete an image

1. From the **Manage > Azure Quick Deploy** dashboard, expand **Master Images** on the right.
2. Click the image you want to delete.
3. Click **Delete Image** at the bottom of the card. Confirm the deletion.

Install a Windows VDA on an image

Use the following procedure when preparing a Windows image that you plan to import into Citrix DaaS for Azure. For Linux VDA installation guidance, see the Linux VDA product documentation.

1. In your Azure environment, connect to the image VM (if you're not already connected).
2. You can download a VDA by using the **Downloads** link on the Citrix Cloud navigation bar. Or, use a browser to navigate to Citrix DaaS for Azure download page.

Download a VDA onto the VM. There are separate VDA download packages for a desktop (single-session) OS and a server (multi-session) OS.

3. Launch the VDA installer by double-clicking the downloaded file. The installation wizard launches.
4. On the **Environment** page, select the option to create an image using MCS, and then click **Next**.
5. On the **Core Components** page, click **Next**.
6. On the **Delivery Controller** page, select **Let Machine Creation Services do it automatically** and then click **Next**.
7. Leave the default settings on the **Additional Components**, **Features**, and **Firewall** pages, unless Citrix instructs you otherwise. Click **Next** on each page.
8. On the **Summary** page, click **Install**. Prerequisites begin to install. When prompted to restart, agree.
9. The VDA installation resumes automatically. Prerequisite installation completes and then the components and features are installed. On the **Call Home** page, leave the default setting (unless Citrix instructs you otherwise). After you connect, click **Next**.
10. Click **Finish**. The machine restarts automatically.
11. To ensure that the configuration is correct, launch one or more of the applications you installed on the VM.
12. Shut down the VM. Do not Sysprep the image.

For more information about installing VDAs, see Install VDAs.

Users and authentication

September 26, 2023

User authentication methods

Users must authenticate when they log in to Citrix Workspace to start their desktop or apps.

Citrix DaaS for Azure supports the following user authentication methods:

- **Managed Azure AD:** Managed Azure AD is an Azure Active Directory (AAD) provided and managed by Citrix. You don't need to provide your own Active Directory structure. Just add your users to the directory.

- **Your identity provider:** You can use any available authentication method in Citrix Cloud.

> **Note:**
>
> - Remote PC Access deployments use only Active Directory. For details, see Remote PC Access.
> - If you use Azure AD Domain Services: Workspace logon UPNs must contain the domain name that was specified when enabling Azure AD Domain Services. Logons cannot use UPNs for a custom domain you create, even if that custom domain is designated as primary.

Setting up user authentication includes the following procedures:

1. Configure the user authentication method in Citrix Cloud and Workspace Configuration.
2. If you're using Managed Azure AD for user authentication, add users to the directory.
3. Add users to a catalog.

Configure user authentication in Citrix Cloud

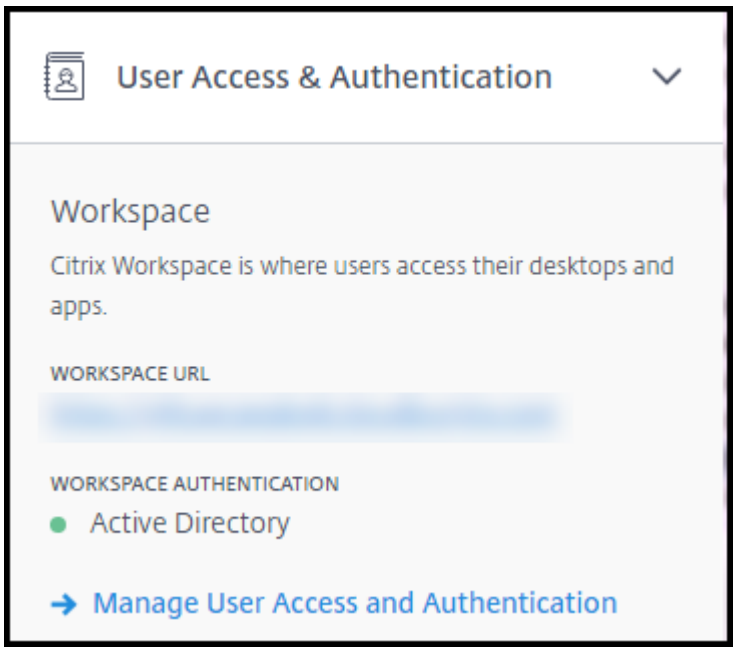
To configure user authentication in Citrix Cloud:

- Connect to the user authentication method you want to use. (In Citrix Cloud, you "connect"or "disconnect"from an authentication method.)
- In Citrix Cloud, set Workspace authentication to use the connected method.

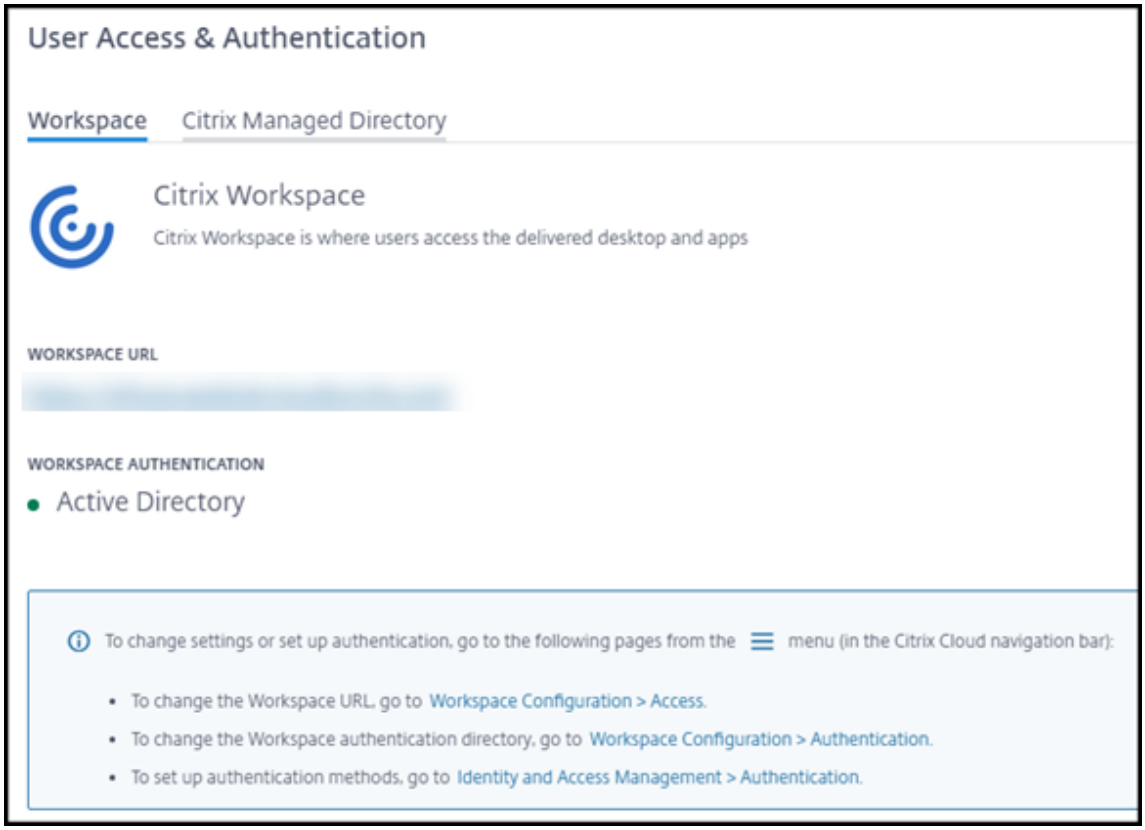
> **Note:**
>
> The Managed Azure AD authentication method is configured by default. That is, it is automatically connected in Citrix Cloud, and Workspace authentication is automatically set to use Managed Azure AD for Citrix DaaS for Azure. If you want to use this method (and have not previously configured a different method), continue with Add and delete users in Managed Azure AD.
> If the Managed Azure AD is disconnected, the Workspace authentication will be switched to Active Directory. If you want to use a different authentication method follow the steps below.

To change the authentication method:

1. From the **Manage > Azure Quick Deploy** dashboard in Citrix DaaS for Azure, click **User Access & Authentication** on the right.



2. Click **Manage User Access and Authentication**. Select the **Workspace** tab, if it isn't already selected. (The other tab indicates which user authentication method is currently configured.)



3. Follow the link **To set up authentication methods**. That link takes you to Citrix Cloud. Select **Connect** in the ellipsis menu for the method you want.

4. While still in Citrix Cloud, select **Workspace Configuration** in the upper left menu. On the **Authentication** tab, select the method you want.

What to do next:

- If you're using Managed Azure AD, add users to the directory.
- For all authentication methods, add users to the catalog.

Add and delete users in Managed Azure AD

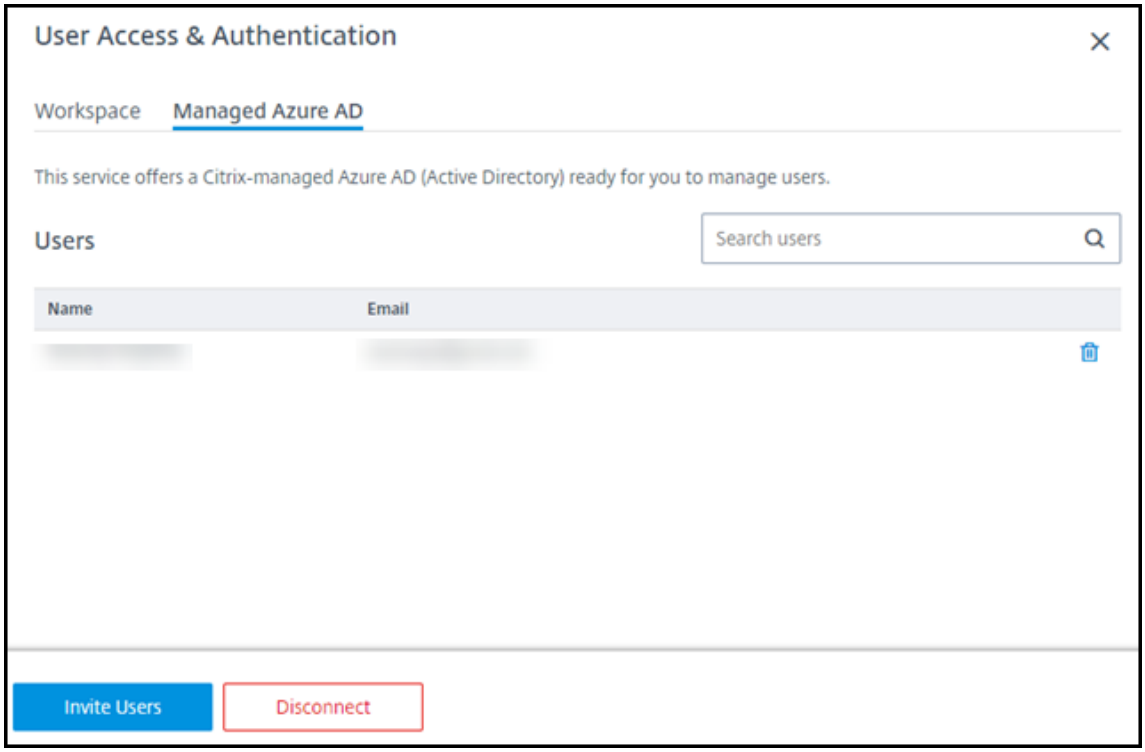
Complete this procedure only if you're using Managed Azure AD for user authentication to Citrix Workspace.

You provide your users'name and email addresses. Citrix then emails an invitation to each of them. The email instructs users to click a link that joins them to the Citrix Managed Azure AD.

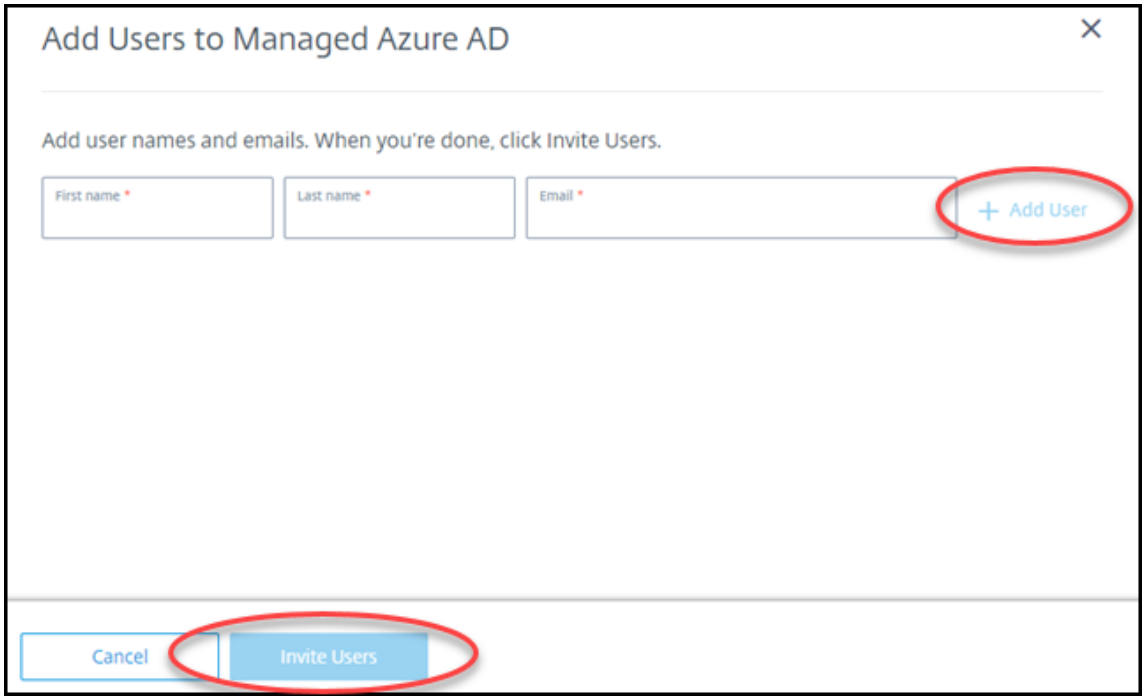
- If the user already has a Microsoft account with the email address you provided, that account is used.
- If the user does not have a Microsoft account with the email address, Microsoft creates an account.

To add and invite users to Managed Azure AD:

1. From the **Manage > Azure Quick Deploy** dashboard in Citrix DaaS for Azure, expand **User Access & Authentication** on the right. Click **Manage User Access and Authentication**.
2. Click the **Managed Azure AD** tab.
3. Click **Invite Users**.



4. Type the name and email address of a user, and then click **Add User**.



5. Repeat the preceding step to add other users.
6. When you're done adding user information, click **Invite Users** at the bottom of the card.

To delete a user from Managed Azure AD, click the trash icon next to the name of the user you want to

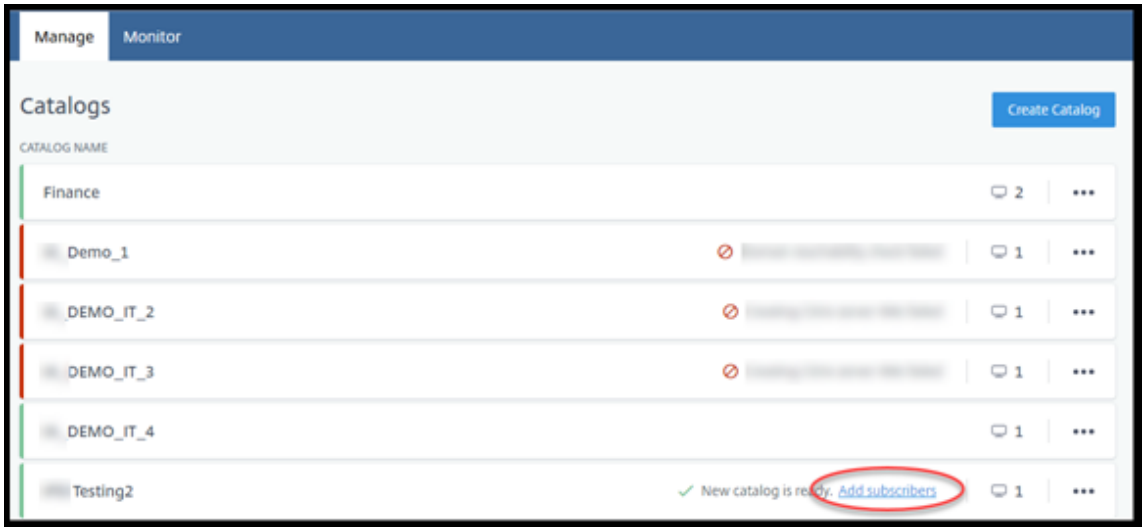
delete from the directory. Confirm the deletion.

What to do next: Add users to the catalog

Add or remove users in a catalog

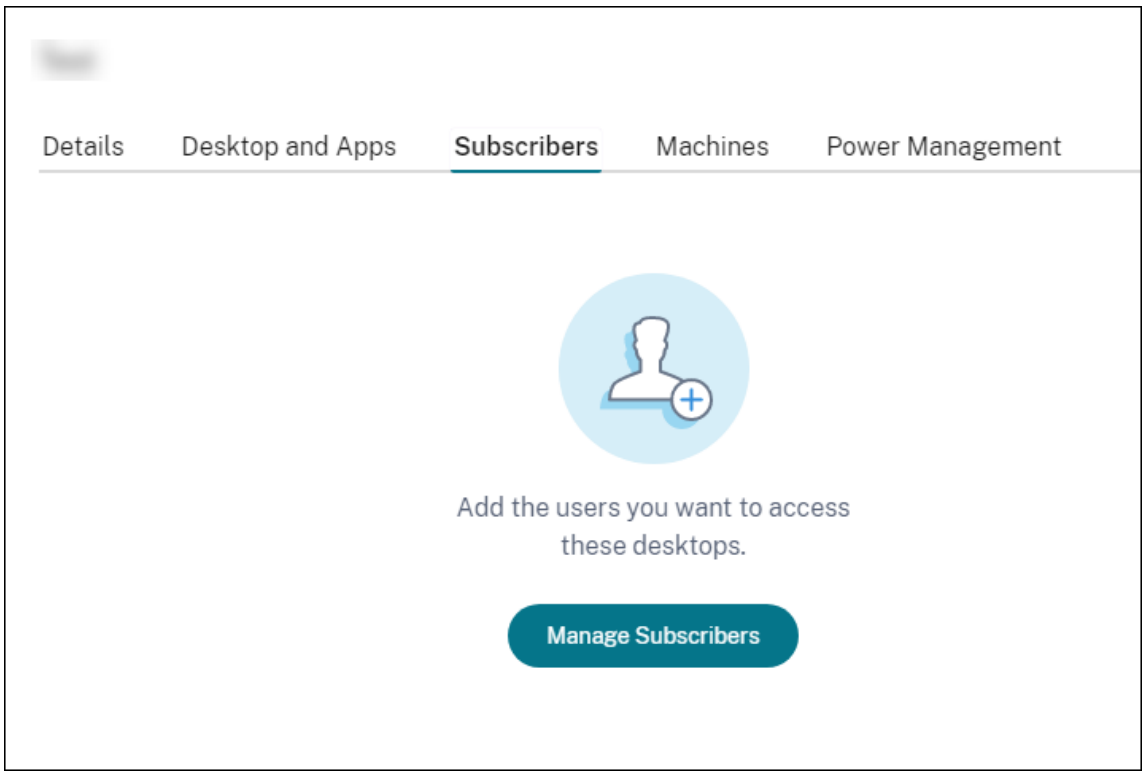
Complete this procedure regardless of which authentication method you use.

1. From the **Manage > Azure Quick Deploy** dashboard in Citrix DaaS for Azure, if you haven't added any users to a catalog, click **Add subscribers**.

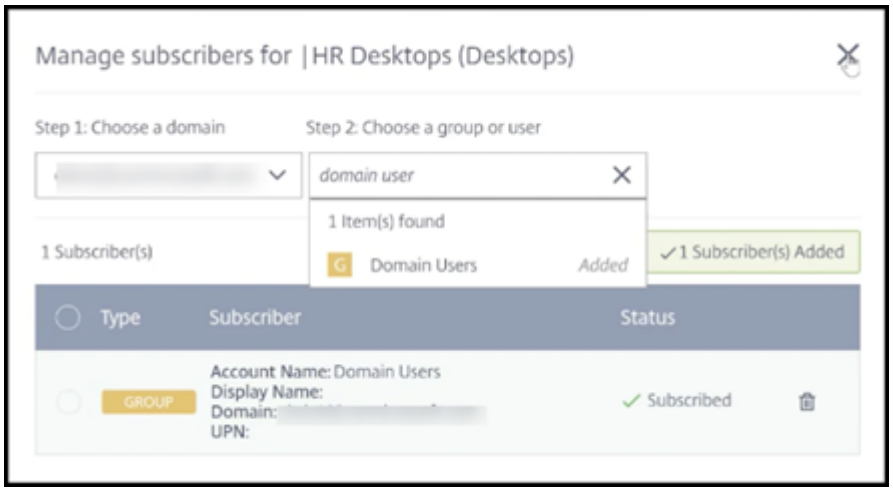


   To add users to a catalog that already has users, click anywhere in the catalog's entry.

2. On the **Subscribers** tab, click **Manage Subscribers**.



3. Select a domain. (If you're using Managed Azure AD for user authentication, there's only one entry in the domain field.) Then select a user.



4. Select other users, as needed. When you're done, click the **X** in the upper right corner.

To remove users from a catalog, follow steps 1 and 2. In step 3, click the trash icon next to the name you want to delete (instead of selecting a domain and group/user). This action removes the user from the catalog, not from the source (such as Managed Azure AD or your own AD or AAD).

What to do next:

- For a catalog with multi-session machines, add applications, if you haven't already.

- For all catalogs, send the Citrix Workspace URL to your users.

More information

For more information about authentication in Citrix Cloud, see Identity and access management.

Manage catalogs

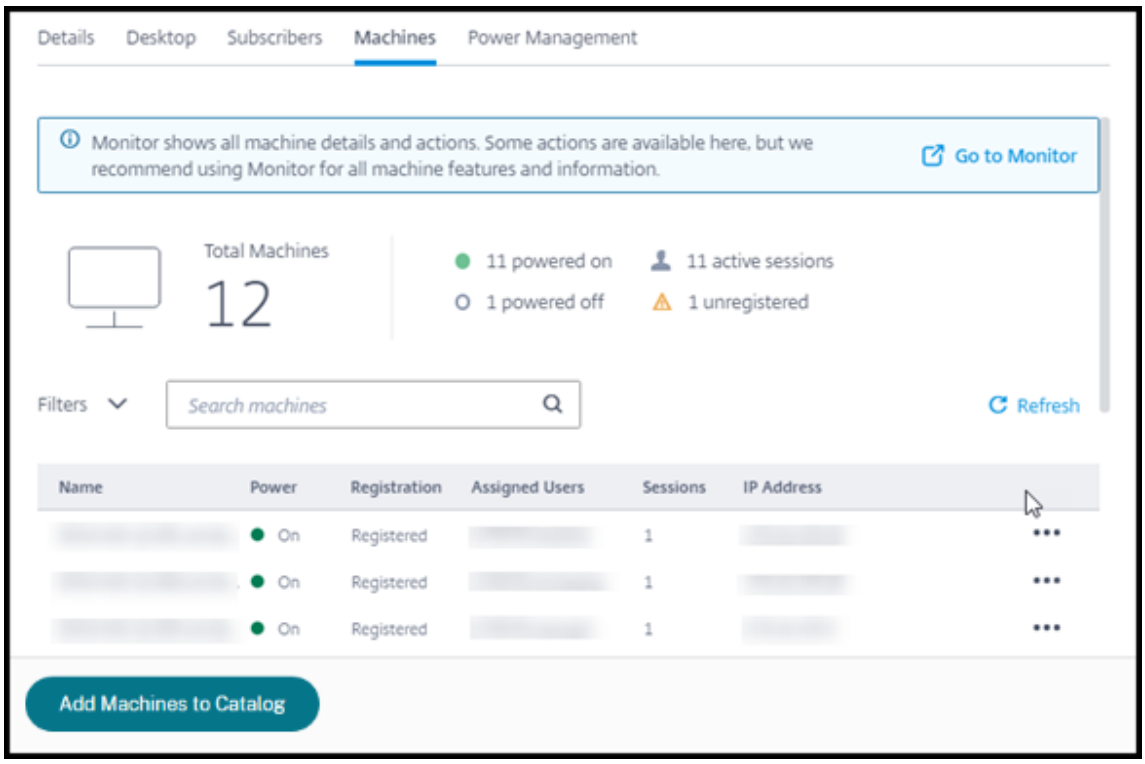
August 30, 2022

> **Note:**
>
> This article describes the tasks you can use to manage catalogs that were created in the Quick Deploy interface. For information about catalog management using the Full Configuration management interface, see Manage machine catalogs.

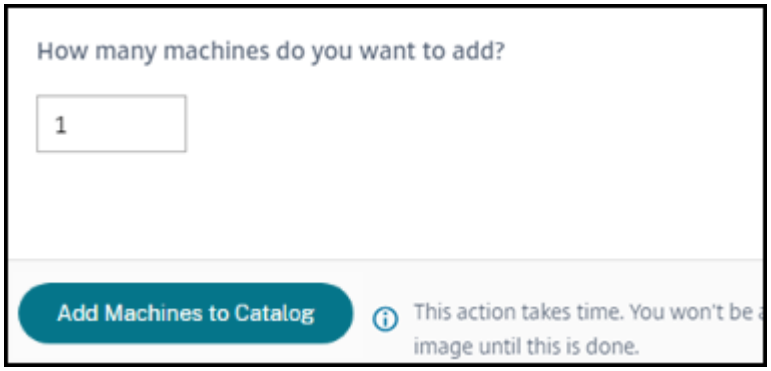
Add machines to a catalog

While machines are being added to a catalog, you cannot make any other changes to that catalog.

1. From the **Manage > Azure Quick Deploy** dashboard, click anywhere in the catalog's entry.
2. On the **Machines** tab, click **Add Machines to Catalog**.



3. Enter the number of machines you want to add to the catalog.



4. (Valid only if the catalog is domain-joined.) Type the user name and password for the service account.
5. Click **Add Machines to Catalog**.

You cannot reduce the machine count for a catalog. However, you can use power management schedule settings to control how many machines are powered on, or delete individual machines from the **Machines** tab. See Manage machines in a catalog for information on deleting machines from the **Machines** tab.

Change the number of sessions per machine

Changing the number of sessions per multi-session machine can affect users'experience. Increasing this value can reduce the compute resources allocated to concurrent sessions. Recommendation: Observe your usage data to determine the appropriate balance between user experience and cost.

1. From the **Manage > Azure Quick Deploy** dashboard, select a catalog containing multi-session machines.
2. On the **Details** tab, click **Edit** next to **Sessions per Machine**.
3. Enter a new number of sessions per machine.
4. Click **Update Number of Sessions**.
5. Confirm your request.

This change does not affect current sessions. When you change the maximum number of sessions to a value that is lower than a machine's currently active sessions, the new value is implemented through the normal attrition of active sessions.

If a failure occurs before the update process begins, the catalog's **Details** display retains the correct number of sessions. If a failure occurs during the update process, the display indicates the number of sessions you wanted.

Manage machines in a catalog

> **Note:**
>
> Many of the actions that are available from the **Manage > Azure Quick Deploy** dashboard are also available from the **Monitor** dashboard in Citrix DaaS Standard for Azure (formerly Citrix Virtual Apps and Desktops Standard for Azure service).

To select actions from the **Manage > Azure Quick Deploy** dashboard:

1. From the **Manage > Azure Quick Deploy** dashboard, click anywhere in a catalog's entry.
2. On the **Machines** tab, find the machine you want to manage. In the ellipsis menu for that machine, select the desired action:
   - **Restart:** Restart the selected machine.
   - **Start:** Start the selected machine. This action is available only if the machine is powered off.
   - **Shutdown:** Shut down the selected machine. This action is available only if the machine is powered on.
   - **Turn maintenance mode on/off:** Turn maintenance mode on (if it is off) or off (if it is on) for the selected machine.

By default, maintenance mode is turned off for a machine. Turning on maintenance mode for a machine prevents new connections from being made to that machine. Users can connect to existing sessions on that machine, but they cannot start new sessions on that machine. You might place a machine in maintenance mode before applying patches, or for troubleshooting.

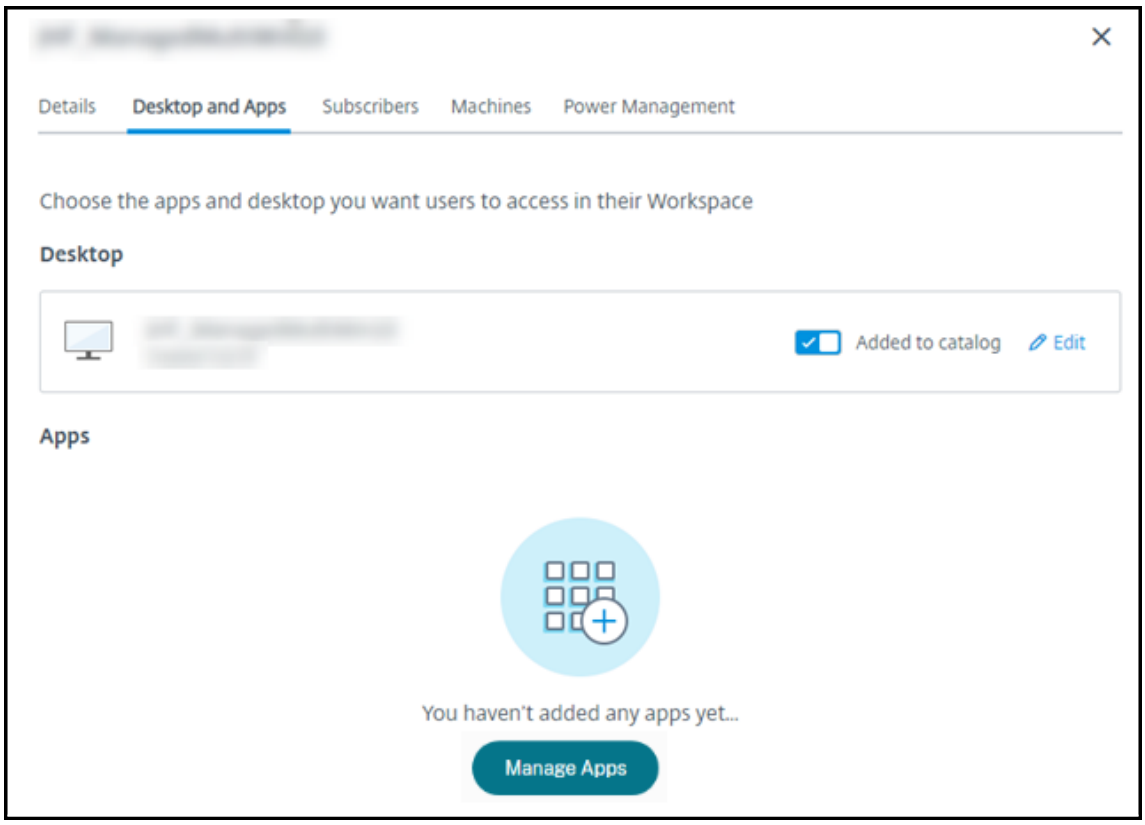
- **Delete:** Delete the selected machine. This action is available only when the machine's session count is zero. Confirm the deletion.

  When a machine is deleted, all data on the machine is removed.

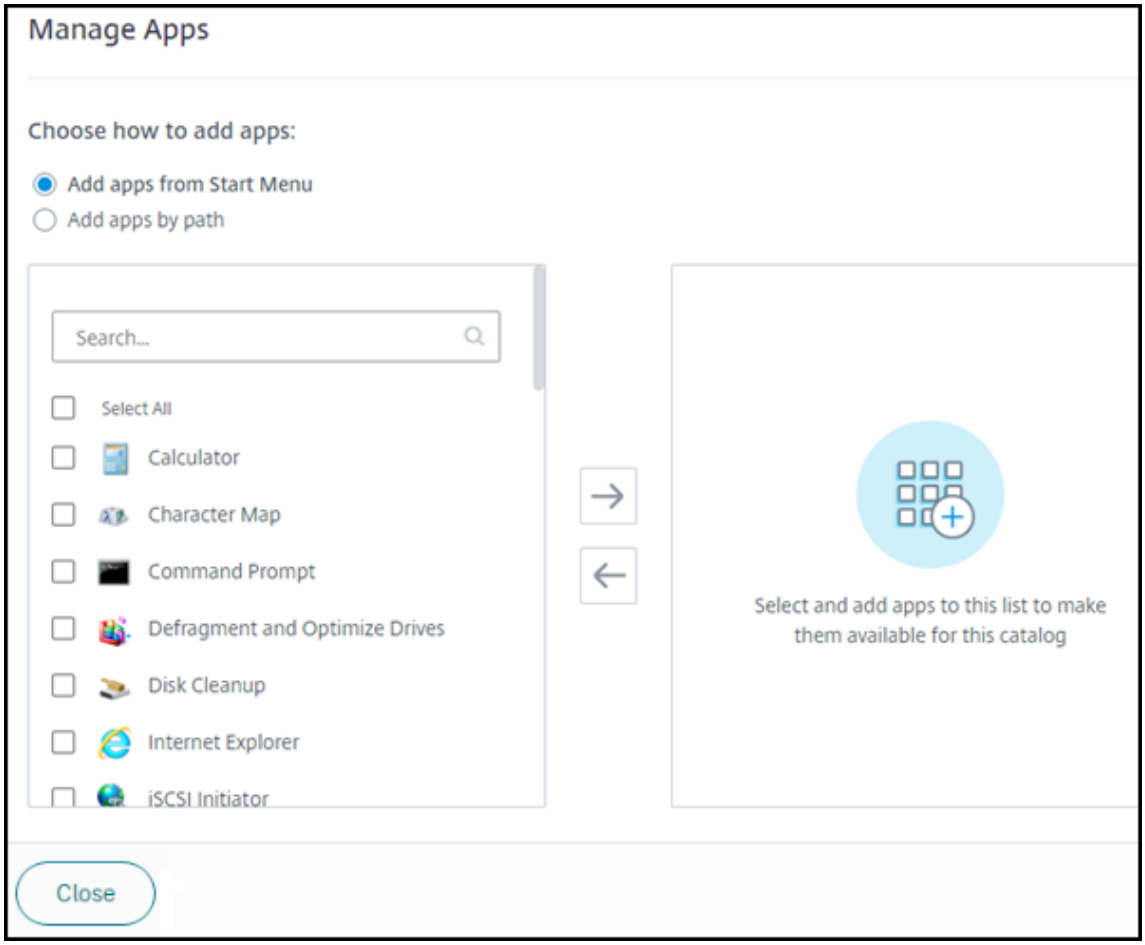
- **Force restart:** Force a restart of the selected machine. Select this action only if a **Restart** action for the machine failed.

Add apps to a catalog

1. From the **Manage > Azure Quick Deploy** dashboard, click anywhere in the catalog's entry.
2. On the **Desktop and Apps** tab, click **Manage Apps**.

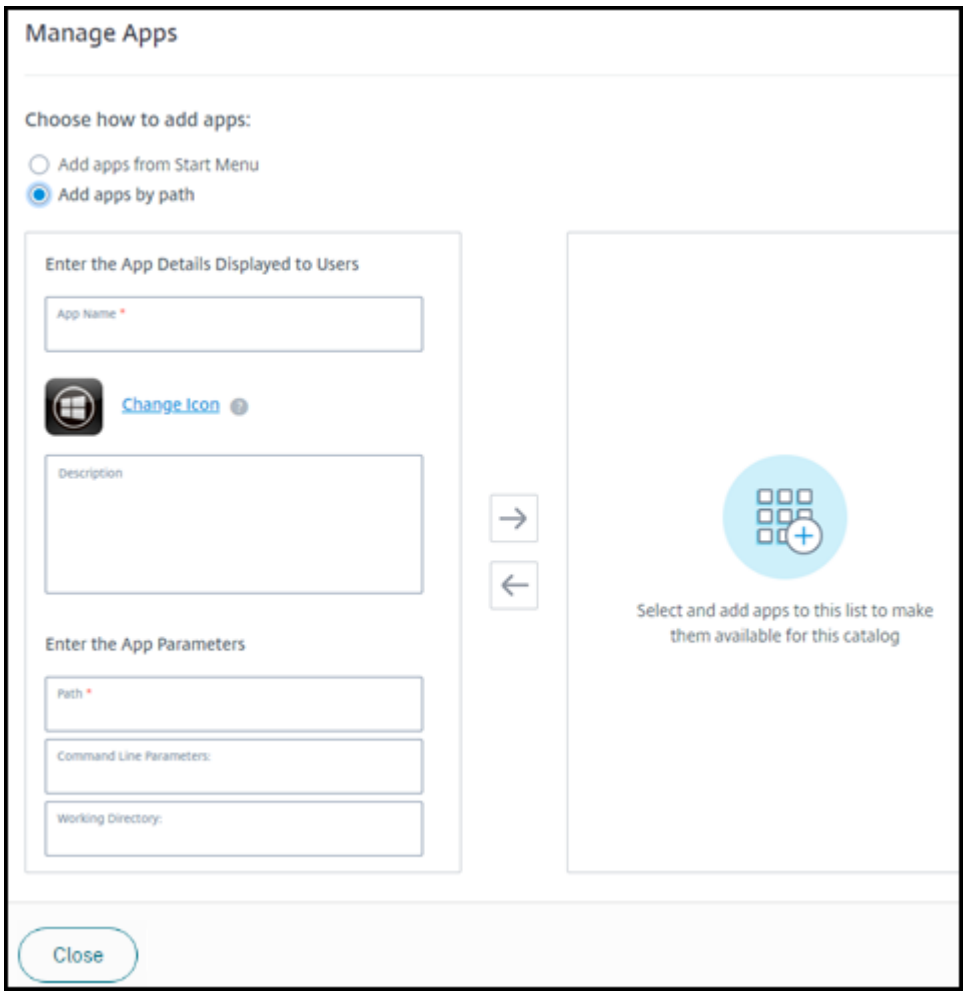


3. Select how you are adding apps: from the **Start** menu of machines in the catalog, or from a different path on the machines.
4. To add apps from the **Start** menu:



- Select available apps in the left column. (Use **Search** to tailor the apps list.) Click the right arrow between the columns. The selected apps move to the right column.
- Similarly, to remove apps, select them in the right column. Click the left arrow between columns.
- If the **Start** menu has more than one version of the same app, with the same name, you can add only one. To add another version of that app, edit that version to change its name. Then you can add that version of the app.

5. To add apps by path:



- Enter the name for the app. This is the name users see in Citrix Workspace.
- The icon shown is the icon users see in Citrix Workspace. To select another icon, click **Change icon** and navigate to the icon you want to display.
- (Optional) Enter a description of the application.
- Enter the path to the app. This field is required. Optionally, add command line parameters and the working directory. For details about command line parameters, see Pass parameters to published applications.

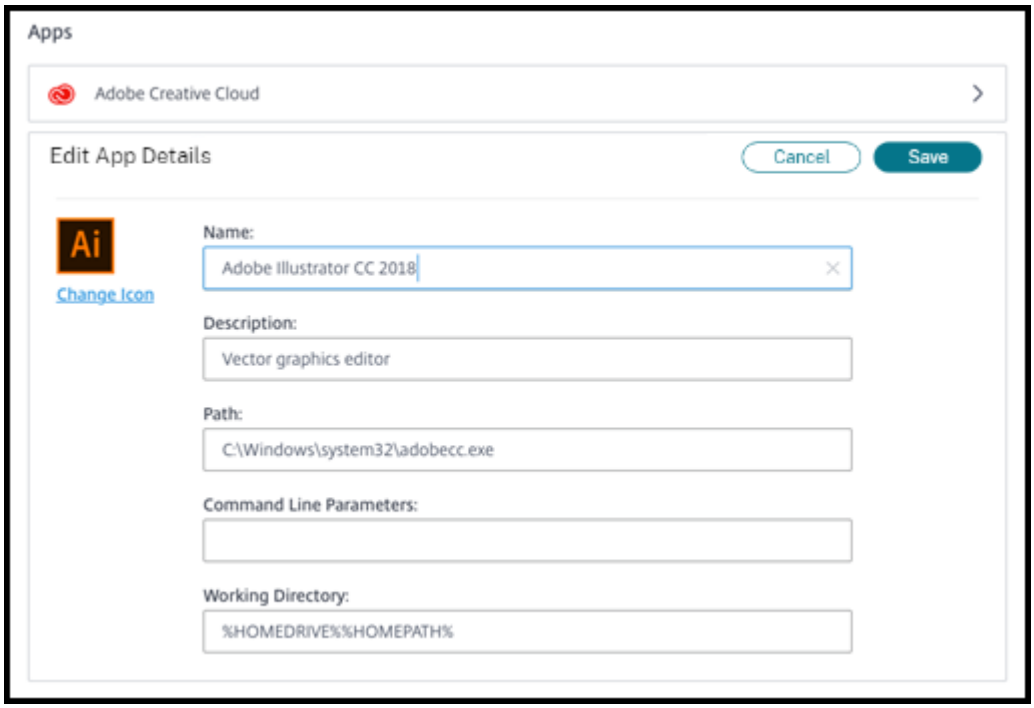
6. When you're finished, click **Close**.

What to do next (if you're completing the catalog creation and delivery flow): Send the Citrix Workspace URL to your users, if you haven't already.

On Windows Server 2019 VDAs, some application icons might not appear correctly during configuration and in the users'workspace. As a workaround, after the app is published, edit the app and use the **Change icon** feature to assign a different icon that displays correctly.

Edit an app in a catalog

1. From the **Manage > Azure Quick Deploy** dashboard, click anywhere in the catalog's entry.
2. On the **Desktop and Apps** tab, click anywhere on the row containing the app you want to edit.
3. Click the pencil icon.



4. Type changes in any of the following fields:
   - **Name:** The name users see in Citrix Workspace.
   - **Description**
   - **Path:** The path to the executable.
   - **Command line parameters:** For details, see Pass parameters to published applications.
   - **Working directory**
5. To change the icon users see in their Citrix Workspace, click **Change icon** and navigate to the icon you want to display.
6. When you're done, click **Save**.

Pass parameters to published applications

When you associate a published application with file types, the percent and star symbols (enclosed in double quotation marks) are appended to the end of the command line. These symbols act as a placeholder for parameters passed to user devices.

- If a published application does not launch when expected, verify that its command line contains the correct symbols. By default, parameters supplied by user devices are validated when the symbols are appended.

  For published applications that use customized parameters supplied by the user device, the symbols are appended to the command line to bypass command-line validation. If you do not see these symbols in a command line for the application, add them manually.

- If the path to the executable file includes directory names with spaces (such as "C:\Program Files"), enclose the command line for the application in double quotation marks to indicate that the space belongs in the command line. Add double quotation marks around the path, and another set of double quotation marks around the percent and star symbols. Add a space between the closing quotation mark for the path and the opening quotation mark for the percent and star symbols.

  For example, the command line for the published application Windows Media Player is: `" C:\Program Files\Windows Media Player\mplayer1.exe" "%*"`

Remove apps from a catalog

Removing an app from a catalog does not remove it from the machines. It just prevents it from appearing in Citrix Workspace.

1. From the **Manage > Azure Quick Deploy** dashboard, click anywhere in the catalog's entry.
2. On the **Desktop and Apps** tab, click the trash icon next to the apps you want to remove.

Delete a catalog

When you delete a catalog, all the machines in the catalog are permanently destroyed. Deleting a catalog cannot be reversed.

1. From the **Manage > Azure Quick Deploy** dashboard, click anywhere in the catalog's entry.
2. On the **Details** tab, click **Delete Catalog** on the lower portion of the window.
3. Confirm the deletion by selecting the acknowledgment check boxes and then clicking the confirmation button.

To help identify residual Active Directory machine accounts that you must delete, you can download a list of machine and Cloud Connector names.

Manage power management schedules

A power management schedule affects all machines in a catalog. A schedule provides:

- Optimal user experience: Machines are available for users when they're needed.
- Security: Desktop sessions that remain idle for a specified interval are disconnected, requiring users to launch a new session in their workspace.
- Cost management and power savings: Machines with desktops that remain idle are powered-off. Machines are powered on to meet scheduled and actual demand.

You can configure a power schedule when you create a custom catalog or do it later. If no schedule is selected or configured, a machine powers off when a session ends.

You cannot select or configure a power schedule when creating a catalog with quick create. By default, quick create catalogs use the Cost Saver preset schedule. You can select or configure a different schedule later for that catalog.

Schedule management includes:

- Knowing what information a schedule contains
- Creating a schedule

Information in a schedule

The following diagram shows the schedule settings for a catalog containing multi-session machines. Settings for a catalog containing single-session (random or static) machines differ slightly.

A power management schedule contains the following information.

Preset schedules Citrix DaaS for Azure offers several preset schedules. You can also configure and save custom schedules. Although you can delete custom presets, you cannot delete Citrix-provided presets.

Time zone Used with the power-on machines setting to establish work hours and after hours, based on the selected time zone.

This setting is valid for all machine types.

Power on machines: Work hours and after hours The days of the week and start-stop hours of the day that form your work hours. This generally indicates the intervals when you want machines powered on. Any time outside of those intervals is considered after-hours. Several schedule settings allow you to enter separate values for work hours and after-hours. Other settings apply all the time.

This setting is valid for all machine types.

Disconnect desktop sessions when idle How long a desktop can remain idle (not used) before the session is disconnected. After a session is disconnected, the user must go to Workspace and start a desktop again. This is a security setting.

This setting is valid for all machine types. One setting applies all the time.

Power off idle desktops How long a machine can remain disconnected before it is powered off. After a machine is powered off, the user must go to Workspace and start a desktop again. This is a power-saving setting.

For example, let's say you want desktops to disconnect after they have been idle for 10 minutes. Then, power off the machines if they remain disconnected for another 15 minutes.

If Tom stops using his desktop and walks away for a one-hour meeting, the desktop will be disconnected after 10 minutes. After another 15 minutes, the machine will be powered off (25 minutes total).

From a user standpoint, the two idle settings (disconnect and power-off) have the same effect. If Tom stays away from his desktop for 12 minutes or an hour, he must start a desktop again from Workspace. The difference in the two timers affects the state of the virtual machine providing the desktop.

This setting is valid for single-session (static or random) machines. You can enter values for work hours and after-hours.

Log off disconnected sessions How long a machine can remain disconnected before the session is closed.

This setting is valid for multi-session machines. One setting applies all the time.

Power-off delay The minimum amount of time a machine must be powered-on before it is eligible for power-off (along with other criteria). This setting keeps machines from "flip-flopping"on and off during volatile session demands.

This setting is valid for multi-session machines, and applies all the time.

Minimum running machines How many machines must remain powered-on, regardless of how long they are idle or disconnected.

This setting is valid for random and multi-session machines. You can enter values for work hours and after-hours.

Capacity buffer A capacity buffer helps accommodate sudden spikes in demand, by keeping a buffer of machines powered-on. The buffer is specified, as a percentage of current session demand. For example, if there are 100 active sessions and the capacity buffer is 10%, Citrix DaaS for Azure provides capacity for 110 sessions. A spike in demand might occur during work hours or adding new machines to the catalog.

A lower value decreases the cost. A higher value helps ensure an optimized user experience. When launching sessions, users do not have to wait for extra machines to power on.

When there are more than enough machines to support the number of powered-on machines needed in the catalog (including the capacity buffer), extra machines are powered off. Power-off might occur because of off-peak time, session logoffs, or fewer machines in the catalog. The decision to power off a machine must meet the following criteria:

- The machine is powered on and not in maintenance mode.
- The machine is registered as available or waiting to register after power-on.
- The machine has no active sessions. Any remaining sessions have ended. (The machine was idle for the idle timeout period.)
- The machine has been powered on for at least "X"minutes, where "X"is the power-off delay specified for the catalog.

  In a static catalog, after all machines in the catalog are assigned, the capacity buffer does not play a role in powering machines on or off.

This setting is valid for all machine types. You can enter values for work hours and after-hours.

Create a power management schedule

1. From the **Manage > Azure Quick Deploy** dashboard, click anywhere in the catalog's entry.

2. On the **Power Management** tab, determine whether any of the preset schedules (in the menu at the top) meet your needs. Select a preset to see the values it uses. If you want to use a preset, leave it selected.
3. If you change the values in any fields (such as days, times, or intervals), the preset selection changes to **Custom** automatically. An asterisk indicates that custom settings have not been saved.
4. Set the values you want for the custom schedule.
5. Click **Custom** at the top and save the current settings as a new preset. Enter a name for the new preset and click the check mark.
6. When you're done, click **Save Changes**.

Later, you can edit or delete a custom preset by using the pencil or trash icons in the **Presets** menu. You cannot edit or delete common presets.

VDA snapshot and restore

The Citrix DaaS for Azure snapshot and restore features provide a way to recover from unplanned data loss or other failures in VDAs that deliver desktops and apps. The snapshot operation takes and stores a snapshot of the machine. Later, a restore operation uses a snapshot you select.

- You can configure daily and weekly snapshot schedules for all the machines in a catalog. These snapshots are called *automatic snapshots*. A snapshot is taken of each machine in the catalog. There are no default snapshot schedules.
- You can back up a single V in a catalog on demand. This is called a manual snapshot. You can create a *manual snapshot* of a machine even if the catalog it belongs to has scheduled snapshots. (However, you can't schedule single-machine snapshots.)

> **Important:**
>
> The Citrix DaaS for Azure snapshot and restore features are supported only for machines in static catalogs and assigned to users.

Snapshot schedules

Remember: Snapshot schedules apply to all machines in a catalog.

By default, there are no snapshot schedules.

To manage snapshot schedules:

1. From the **Manage** dashboard, click anywhere in the catalog's entry.
2. On the **Details** tab, click **Schedule Snapshots**.

3. On the **Schedule Snapshots** page, configure schedules for weekly or daily automatic snapshots, or both:
    - To add or change weekly snapshots, move the slider for **Weekly automatic snapshots** until a check mark appears. Select the day of the week and the start time.
    - To add or change daily snapshots, move the slider for **Daily automatic snapshots** until a check mark appears. Select the start time.
    - To remove weekly snapshots, move the slider for **Weekly automatic snapshots** until an **X** appears.
    - To remove daily snapshots, move the slider for **Daily automatic snapshots** until an **X** appears.
4. When you're done, click **Save** at the bottom of the page.

Manual snapshots

A manual snapshot is for a single machine in a catalog. (You cannot create a schedule to take a snapshot of single machines.)

1. From the **Manage** dashboard, click anywhere in the catalog's entry.
2. On the **Machines** tab, find the machine you want to take a snapshot of. Select **Snapshots** in the ellipsis menu for that machine.
3. On the **Snapshots for *VDA-name*** page, click **Create Manual Snapshot**.
4. Provide a name for the snapshot. Recommended: Choose a name you can easily identify later.
5. Confirm your request.

View and manage snapshots

1. From the **Manage** dashboard, click anywhere in the catalog's entry.
2. On the **Machines** tab, find the machine you want to take a snapshot of. Select **Snapshots** in the ellipsis menu for that machine.
3. On the **Backups for *VDA-name*** page:
    - If there are no snapshots for the machine, a message guides you to either create a manual snapshot for this machine, or create scheduled snapshots for all of the machines in the catalog containing this machine.
    - You can select one of the snapshots and restore the machine. See Restore.
    - You can delete snapshots. Select the check boxes for one or more snapshots and then click **Delete** in the table header. Confirm your request.

Tip: When you delete a catalog, all snapshots are destroyed.

Restore

You can restore a machine from any available snapshot for that machine.

During a restore, the machine is powered off. None of the actions in a machine's ellipsis menu are available while a snapshot is being restored.

1. From the **Manage** dashboard, click anywhere in the catalog's entry.
2. On the **Machines** tab, find the machine you want to take a snapshot of. Select **Snapshots** in the ellipsis menu for that machine.
3. On the **Snapshots for *VDA-name page***, select the check box of the snapshot you want to use.
4. Click **Restore** in the table header.
5. Confirm the request.

The **Status** column on the **Machines** tab indicates the progress and outcome of the restore operation.

If a machine fails to restore a snapshot, try again.

Related information

- Update a catalog with a new image
- Add and remove users in a catalog
- Domain-joined and non-domain-joined

Monitor

April 10, 2023

From the **Monitor** dashboard, you can view desktop usage, sessions, and machines in your Citrix DaaS Standard for Azure (formerly Citrix Virtual Apps and Desktops Standard for Azure) deployment. You can also control sessions, power-manage machines, end running applications, and end running processes.

To access the **Monitor** dashboard:

1. Sign in to Citrix Cloud, if you haven't already. In the upper left menu, select **My Services > DaaS Standard for Azure**.
2. From the **Manage** dashboard, click the **Monitor** tab.

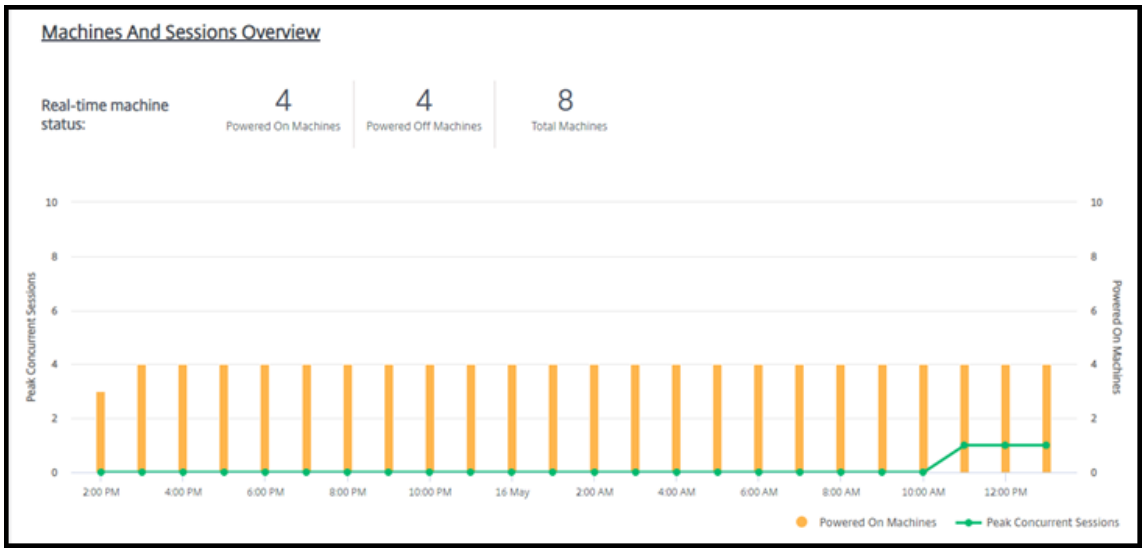
Monitor desktop usage

Displays on this page refresh every five minutes.

- **Machine and Sessions Overview:** You can tailor the display to show information about all catalogs (default) or a selected catalog. You can also tailor the time period: the last day, week, or month.

  Counts at the top of the display indicate the total number of machines, plus the number of machines that are powered-on and powered-off. Hover over a value to display how many are single-session and multi-session.

  The graph below the counts shows the number of powered-on machines and peak concurrent sessions at regular points during the time period you selected. Hover on a point the graph to display the counts at that point.



- **Top 10s:** To tailor a top 10 display, select a time period: the past week (default), month, or three months. You can also tailor the display to show only information about activity involving single-session machines, multi-session machines, or applications.

  - **Top 10 Active Users:** Lists the users who started desktops most frequently during the time period. Hovering on a line displays the total launches.
  - **Top 10 Active Catalogs:** Lists the catalogs with the longest duration during the selected time period. Duration is the sum of all user sessions from that catalog.

Desktop usage report

To download a report containing information about machine launches during the last month, click **Launch Activity**. A message indicates that the request is being processed. The report downloads automatically to the default download location on the local machine.

Filter and search to monitor machines and sessions

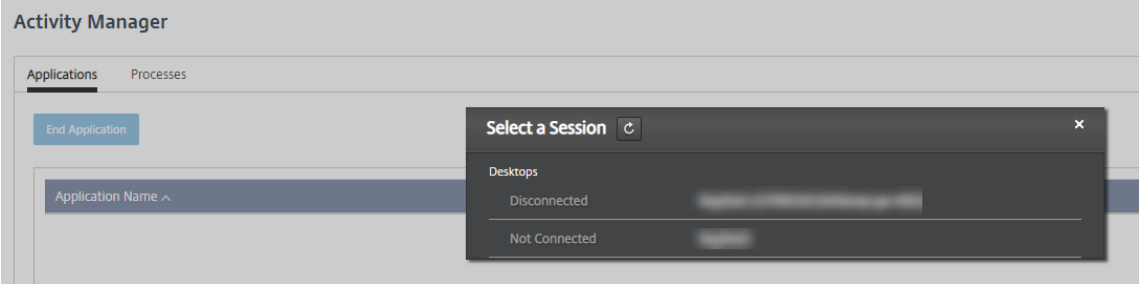
When you're monitoring session and machine information, all machines or sessions are displayed by default. You can:

- Filter the display by machines, sessions, connections, or applications.
- Refine the display of sessions or machines by choosing the criteria you want, building a filter by using expressions.
- Save the filters that you build, for reuse.

Control a user's applications

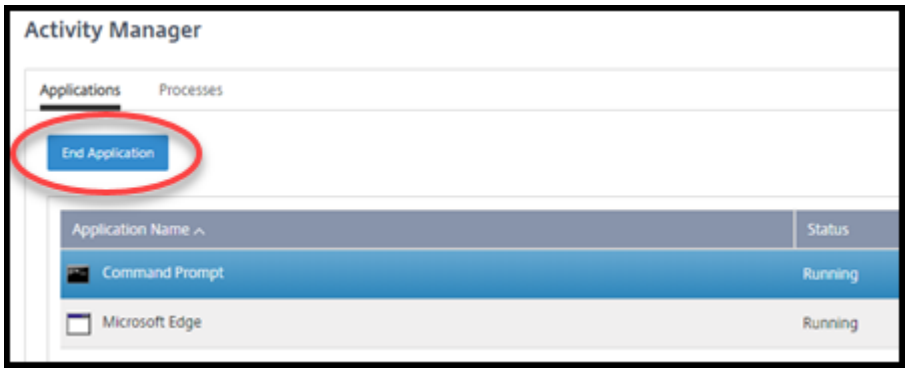
You can display and manage applications and processes for a user that has a running session or an assigned desktop.

1. From the **Monitor** dashboard, click **Search** and enter the user name (or the beginning characters of the user name), machine, or endpoint. From the search results, select the item you're looking for. (To collapse the search box without searching, click **Search** again.)
2. Select a session.



   The Activity Manager lists the applications and processes for the user's session.

3. To end an application, on the **Applications** tab in Activity Manager, click in the application's row to select that application, and then click **End Application**.



4. To end a process, on the **Processes** tab in Activity Manager, click in the process's row to select that process, and then click **End Process**.

5. To display session details, click **Details** in the upper right. To return to the applications and processes display, click Activity Manager in the upper right.
6. To control the session, click **Session Control > Log Off** or **Session Control > Disconnect**.

Shadow users

Use the shadow feature to view or work directly on a user's virtual machine or session. You can shadow Windows and Linux VDAs. The user must be connected to the machine that you want to shadow. Verify this by checking the machine name listed in the `User` title bar.

Shadowing launches in a new browser tab. Ensure that your browser allows pop-ups from the Citrix Cloud URL.

In a Citrix Managed Azure subscription, shadowing is supported only for users on domain-joined machines. To shadow a non-domain-joined machine in a Citrix Managed Azure subscription, you must set up a bastion machine. For details, see Bastion access.

Shadowing must be initiated from a machine on the same virtual network as the domain-joined machines, and also meet any port requirements.

Enable shadowing

1. From the **Monitor** dashboard, go to the **User Details** view.
2. Select the user session, and then click **Shadow** in the **Activity Manager** view or the **Session Details** panel.

Shadow Linux VDAs

Shadowing is available for Linux VDAs Version 7.16 or and later running the RHEL7.3 or Ubuntu Version 16.04 Linux distributions.

Monitor uses the FQDN to connect to the target Linux VDA. Ensure that the Monitor client can resolve the FQDN of the Linux VDA.

- The VDA must have the `python-websockify` and `x11vnc` packages installed.
- `noVNC` connection to the VDA uses the WebSocket protocol. By default, `ws://` WebSocket protocol is used. For security reasons, Citrix recommends that you use the secure `wss://` protocol. Install SSL certificates on each Monitor client and Linux VDA.

Follow the instructions in Session Shadowing to configure your Linux VDA for shadowing.

1. After you enable shadowing, the shadowing connection initializes and a confirmation prompt appears on the user device.

2. Instruct the user to click **Yes** to start the machine or session sharing.
3. The administrator can view only the shadowed session.

Shadow Windows VDAs

Windows VDA sessions are shadowed using Windows Remote Assistance. Enable the `Use Windows Remote Assistance` feature when installing the VDA.

1. After you enable shadowing, the shadowing connection initializes and a dialog box prompts you to open or save the `.msrc incident` file.
2. Open the incident file with the Remote Assistance Viewer, if it's not already selected by default. A confirmation prompt appears on the user device.
3. Instruct the user to click **Yes** to start the machine or session sharing.
4. For more control, ask the user to share keyboard and mouse control.

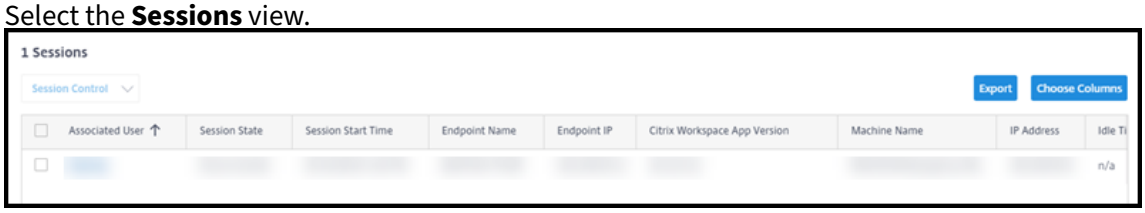
Monitor and control sessions

Session displays are updated every minute.

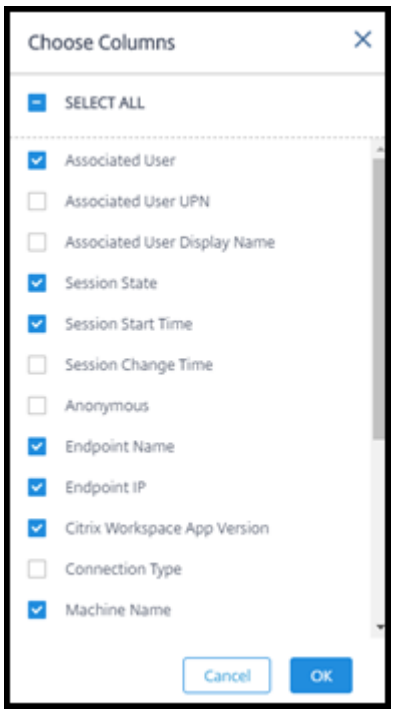
In addition to viewing sessions, you can disconnect one or more sessions or log off users from sessions.

1. From the **Monitor** dashboard, click **Filters**.

2. Select the **Sessions** view.



3. To tailor the display, click **Choose Columns** and select the check boxes of items you want to appear. When you're done, click **OK**. The sessions display refreshes automatically.



4. Click the check box to the left of each session you want to control.
5. To log off or disconnect the session, elect either **Session Control > Log Off** or **Session Control > Disconnect**.

Remember that the power management schedule for the catalog can also control disconnecting sessions and logging off users from disconnected sessions.

As an alternative to the above procedure you can also **Search** for a user, select the session you want to control, and then display session details. The log off and disconnect options are available there, too.

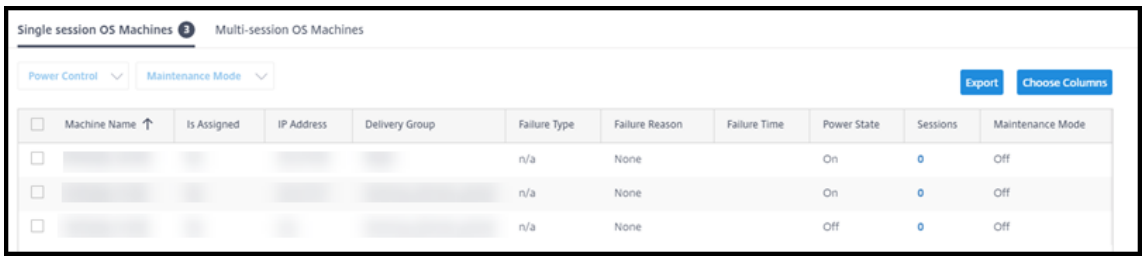
Session information report

To download session information, click **Export** on the sessions display. A message indicates that the request is being processed. The report downloads automatically to the default download location on the local machine.

Monitor and power control machines

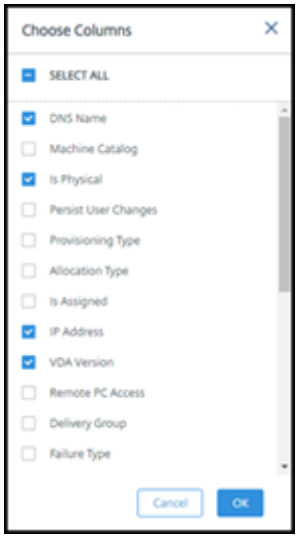
Machine displays are updated every minute.

1. From the **Monitor** dashboard, click **Filters**.
2. Select the **Machines** view.

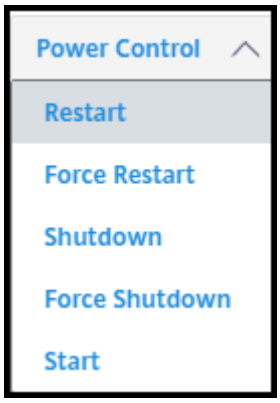


By default, the display lists single-session OS machines. Alternatively, you can display multi-session machines.

3. To tailor the display, click **Choose Columns** and select the check boxes of items you want to appear. When you're done, click **OK**. The machines display refreshes automatically.



4. To power-control machines or place them in or out of maintenance mode, click the check box to the left of each machine you want to control.
5. To power-control the selected machines, click **Power Control** and select an action.



6. To place the selected machines in or out of maintenance mode, click **Maintenance Mode > ON** or **Maintenance Mode > OFF**.

When you use the search feature to find and select a machine, you see machine details, utilization, historical utilization (from the last seven days), and average IOPS.

Machine information report

To download session information, click **Export** on the machines display. A message indicates that the request is being processed. The report downloads automatically to the default download location on the local machine.

Checking app and desktop health

Probing automates the process of checking the health of published apps and desktops. The health check results are available through the **Monitor** dashboard. For details, see:

- Application probing
- Desktop probing

Citrix DaaS for Azure for Citrix Service Providers

August 30, 2022

This article describes how Citrix Service Providers (CSPs) can set up Citrix DaaS Standard for Azure (formerly Citrix Virtual Apps and Desktops Standard for Azure service) for customers (tenants) in Citrix Cloud.

For an overview of the features available for Citrix Partners, see Citrix Cloud for Partners.

Requirements

- You are a Citrix Service Provider partner.
- You have a Citrix Cloud account.
- You have a subscription to Citrix DaaS for Azure.

Limitations

- Customer name changes can take up to 24 hours to apply across all interfaces.
- When creating a customer, the email address must be unique.

Known issues

- After a customer's user is assigned to a resource, you cannot remove or unassign them.
- The management console does not enforce customer user separation. You are responsible for adding users to the appropriate catalogs and resources.

Add a customer

1. Sign in to Citrix Cloud with your CSP credentials. Click **Customers** in the upper left menu.
2. From the **Customer** dashboard, click **Invite or Add**. Provide the requested information.

   If the customer does not have a Citrix Cloud account, adding the customer creates a customer account. Adding the customer also automatically adds you as a full access administrator of that customer's account.
3. If the customer has a Citrix Cloud account:

   a) A Citrix Cloud URL displays, which you copy and send to the customer. For details of this process, see Inviting a customer to connect.
   b) The customer must add you as a full access administrator to their account. See Add administrators to a Citrix Cloud account.

You can add more administrators later and control which customers they can see on the Citrix DaaS for Azure **Manage** and **Monitor** dashboards.

Add Citrix DaaS for Azure to a customer

1. Sign in to Citrix Cloud with your CSP credentials. Click **Customers** in the upper left menu.
2. From the **Customer** dashboard, select **Add Service** in the ellipsis menu for the customer.
3. In **Select a Service to Add**, click **Citrix DaaS Standard for Azure**.
4. Click **Continue**.

After you complete this procedure, the customer is onboarded to your Citrix DaaS for Azure subscription.

When the onboarding completes, a new customer is created automatically in Citrix DaaS for Azure. The customer is visible in **Manage > Quick Deploy**.

Filter resources by customer

You can filter resources by customer on the Citrix DaaS for Azure **Manage > Azure Quick Deploy** dashboard. (By default, all resources are displayed.) When working with resources such as catalogs, ma-

chine images, and Azure subscriptions, you can select specific customer displays to help organize your tenants' resources.

SD-WAN connections are created on a per-customer basis. The customer must have an SD-WAN Orchestrator service entitlement.

- To create an SD-WAN connection for a customer, follow the guidance in Create an SD-WAN connection. On the **Add a network connection** page, select the customer. You can select the SD-WAN connection type box only if that customer has an SD-WAN Orchestrator service entitlement.
- For the connection creation to succeed, the customer must also have an installed Master Control Node (MCN). However, only the SD-WAN Orchestrator service entitlement determines whether the SD-WAN connection type can be selected.

Create catalogs to deliver apps and desktops

A catalog is a group of users and the collection of virtual machines they have access to. When you create a catalog, an image is used (with other settings) as a template for creating the machines. For details, see Create catalogs.

Federated domains

Federated domains enable customer users to use credentials from a domain attached to your resource location to sign in to their workspace. You can provide dedicated workspaces to your customers that their users can access through a custom workspace URL (for example, `customer.cloud.com`), while the resource location remains on your Citrix Cloud account.

You can provide dedicated workspaces alongside the shared workspace that customers can access using your CSP workspace URL (for example, `csppartner.cloud.com`). To enable customer access to their dedicated workspace, you add them to the appropriate domains that you manage.

After configuring the workspace through Workspace Configuration, customers' users can sign in to their workspace and access the apps and desktops that you've made available.

Add a customer to a domain

1. Sign in to Citrix Cloud with your CSP credentials. Click **Customers** in the upper left menu.
2. From the **Customer** dashboard, select **Identity and Access Management** in the upper left menu.
3. On the **Domains** tab, select **Manage Federated Domain** in the domain's ellipsis menu.

4. On the **Manage Federated Domain** card, in the **Available customers** column, select a customer you want to add to the domain. Click the plus sign next to the customer name. The selected customer now appears in the **Federated customers** column. Repeat to add other customers.
5. When you're done, click **Apply**.

Remove a customer from a domain

When you remove a customer from a domain that you manage, the customer's users can no longer access their workspaces using credentials from your domain.

1. From Citrix Cloud, select **Identity and Access Management** in the upper left menu.
2. On the **Domains** tab, select **Manage Federated Domain** from the ellipsis menu for the domain you want to manage.
3. From the list of federated customers, locate or search for the customers you want to remove.

   - Click **X** to remove a customer.
   - To remove all listed customers from the domain, click **Remove all**.

   The selected customers move to the list of **Available customers**.
4. Click **Apply**.
5. Review the customers you selected, and then click **Remove Customers**.

Add an administrator with restricted access

1. Sign in to Citrix Cloud with your CSP credentials. Click **Customers** in the upper left menu.
2. From the **Customer** dashboard, select **Identity and Access Management** in the upper left menu.
3. On the **Administrators** tab, click **Add Administrators From**, and then select **Citrix Identity**.
4. Type the email address of the person you're adding as an administrator, and then click **Invite**.
5. Configure the appropriate access permissions for the administrator. Citrix recommends selecting **Custom access**, unless you want the administrator to have management control of Citrix Cloud and all subscribed services.
6. Select one or more role and scope pairs for Citrix DaaS for Azure, as needed.
7. When you're done, click **Send Invite**.

When the administrator accepts the invitation, they have the access that you assigned.

Partner access to customer identity provider

You can manage users from the Citrix DaaS for Azure **Manage > Azure Quick Deploy** dashboard or the Citrix Cloud console.

When you use a non-AD identity provider for users (such as Citrix Managed Azure AD), you must be a Citrix Cloud Identity and Workspace administrator for the customer before you can manage users for that customer. If you're not an administrator for a customer, you cannot add or delete users for that customer.

To manage users for a customer from **Manage > Azure Quick Deploy** dashboard, select the partner or customer in **Show items for**.

- **Example 1:** Select customer A from **Show items for**. The dashboard now shows only the items for customer A. When you select a catalog, you see only customer A's users on the **Subscribers** tab. You can add or remove users for customer A (assuming you're an administrator for that customer).
- **Example 2:** You select the partner entry in **Show items for**. The dashboard now shows only partner items. On the **Subscribers** tab, you see only users created for the partner. No customer entries appear. You can add or remove users for that partner (assuming you're an administrator of that partner), but you can't manage any customer users from this location.

To manage users for a customer from the Citrix Cloud console, select the customer when prompted after sign-in (or later, using **Change Customer** in the upper right area of the Citrix Cloud console). When using the Library to manage users, the display context reflects the selected customer. For example, if you selected customer A, the Library shows only customer A's offerings.

Edit Delegated Administration permissions for administrators

1. Sign in to Citrix Cloud with your CSP credentials. Click **Customers** in the upper left menu.
2. From the **Customer** dashboard, select **Identity and Access Management** in the upper left menu.
3. On the **Administrators** tab, select **Edit Access** from the ellipsis menu for the administrator.
4. Select or clear the role and scope pairs for Citrix DaaS for Azure, as needed. Be sure to enable only entries that contain the unique scope that was created for the customer.
5. Click **Save**.

Access and configure workspaces

Each customer gets their own workspace with a unique `customer.cloud.com` URL. This URL is where the customer's users access their published apps and desktops.

- **From Citrix DaaS Standard for Azure:** On the **Manage > Azure Quick Deploy** dashboard, view the URL by expanding **User Access & Authentication** on the right.
- **From Citrix Cloud:** From the **Customer** dashboard, select **Workspace Configuration** from the upper left menu. View the URL on the **Access** tab.

You can change access and authentication to a workspace. You can also customize the workspace appearance and preferences. For details, see the following articles:

- Configure workspaces
- Secure workspaces

Monitor a customer's service

The Citrix Daas for Azure **Monitor** dashboard in a CSP environment is essentially the same as a non-CSP environment. See Monitor for details.

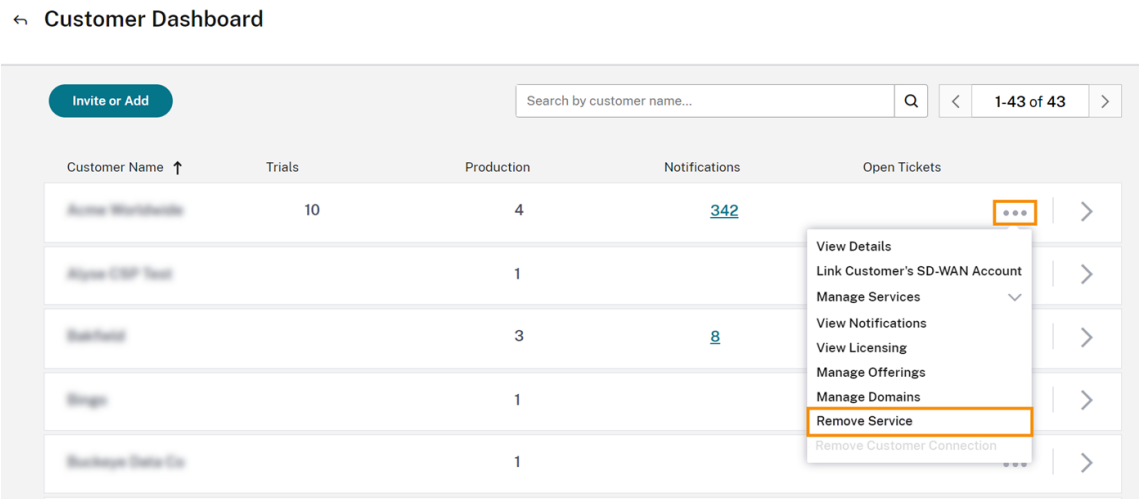
By default, the **Monitor** dashboard displays information about all customers. To display information about one customer, use **Select Customer**.

Keep in mind that the ability to see **Monitor** displays for a customer is controlled by the administrator's configured access.

Remove a Service

Before you begin, ensure that your customer scope is not linked to any Citrix DaaS Standard for Azure objects. If they are linked, you cannot remove the service. To unlink scopes, go to **Citrix Studio > Administrators > Scopes** and edit the scope. For more information about unlinking scopes, see Create and manage scope.

1. Sign in to Citrix Cloud with your Citrix Service Providers credentials.
2. On the **Customer** dashboard, click the ellipsis menu (**...**) of the customer from where you want to remove a service and select **Remove Service**.



The **Service to Remove** page appears.

3. Click **Remove** to remove the service.

Troubleshoot

August 30, 2022

Introduction

Resource locations contain the machines that deliver desktops and apps. Those machines are created in catalogs, so the catalogs are considered part of the resource location. Each resource location also contains Cloud Connectors. Cloud Connectors enable Citrix Cloud to communicate with the resource location. Citrix installs and updates the Cloud Connectors.

Optionally, you can initiate several Cloud Connector and resource location actions. See:

- Resource location actions
- Resource location settings when creating a catalog

Citrix DaaS for Azure has troubleshooting and supportability tools that can help resolve configuration and communication issues with the machines that deliver desktops and apps (the VDAs). For example, creating a catalog might fail, or users might be unable to start their desktop or apps.

This troubleshooting includes gaining access to your Citrix Managed Azure subscription through a bastion machine or direct RDP. After gaining access to the subscription, you can use Citrix supportability tools to locate and resolve issues. For details, see:

- VDA troubleshooting using a bastion or direct RDP
- Bastion access
- Direct RDP access

VDA troubleshooting using a bastion or direct RDP

The supportability features are for people who have experience with troubleshooting Citrix issues. This includes:

- Citrix Service Providers (CSPs) and others who have the technical knowledge and troubleshooting experience with Citrix DaaS products.
- Citrix Support personnel.

If you're not familiar or comfortable with troubleshooting Citrix components, you can request help from Citrix Support. Citrix Support representatives might ask you to set up one of the access methods described in this section. However, the Citrix representatives do the actual troubleshooting, using Citrix tools and technologies.

> **Important:**
>
> These supportability features are valid only for domain-joined machines. If the machines in your catalogs are not domain joined, you're guided to request troubleshooting help from Citrix Support.

Access methods

These access methods are valid only for the Citrix Managed Azure subscription. For more information, see Azure subscriptions.

Two supportability access methods are provided.

- Access your resources through a bastion machine in the customer's dedicated Citrix Managed Azure subscription. The bastion is a single point of entry that allows access to the machines in the subscription. It provides a secure connection to those resources by allowing remote traffic from IP addresses in a specified range.

  The steps in this method include:

  - Create the bastion machine
  - Download an RDP agent
  - RDP to the bastion machine
  - Connect from the bastion machine to the other Citrix machines in your subscription

The bastion machine is intended for short-term use. This method is intended for issues involving the creation of catalogs or image machines.

- Direct RDP access to the machines in the customer's dedicated Citrix Managed Azure subscription. To permit RDP traffic, port 3389 must be defined in the Network Security Group.

  This method is intended for catalog issues other than creation, such as users unable to start their desktops.

Remember: As an alternative to these two access methods, contact Citrix Support for help.

Bastion access

1. From the **Manage > Azure Quick Deploy** dashboard in Citrix DaaS for Azure, expand **Troubleshoot & Support** on the right.
2. Click **View troubleshooting options**.
3. On the **Troubleshoot** page, select either of the first two issue types, and then click **Use our troubleshooting machine**.
4. On the **Troubleshoot with Bastion Machine** page, select the catalog.
   - If the machines in the selected catalog are not domain joined, you're instructed to contact Citrix Support.
   - If a bastion machine has already been created with RDP access to the selected catalog's network connection, skip to step 8.
5. The RDP access range is displayed. If you want to restrict RDP access to a smaller range than allowed by the network connection, select the **Restrict RDP access to only computers in IP address range** check box and then enter the desired range.
6. Type a username and password that you'll use to log in when you RDP to the bastion machine. Password requirements.

   Do not use Unicode characters in the username.
7. Click **Create Bastion Machine**.

   When the bastion machine is successfully created, the page title changes to **Bastion** –***connection***.

   If the bastion machine creation fails (or if it fails during operation), click **Delete** at the bottom of the failure notification page. Try to create the bastion machine again.

   You can change the RDP range restriction after the bastion machine is created. Click **Edit**. Enter the new value and then click the check mark to save the change. (Click **X** to cancel the change.)
8. Click **Download RDP File**.

9. RDP to the bastion, using the credentials you specified when creating the bastion. (The bastion machine's address is embedded in the RDP file you downloaded.)
10. Connect from the bastion machine to the other Citrix machines in the subscription. You can then collect logs and run diagnostics.

Bastion machines are powered on when they are created. To save costs, machines are powered off automatically if they remain idle after startup. The machines are deleted automatically after several hours.

You can power manage or delete a bastion machine, using the buttons at the bottom of the page. If you choose to delete a bastion machine, you must acknowledge that any active sessions on the machine will end automatically. Also, any data and files that were saved on the machine will be deleted.

Direct RDP access

1. From the **Manage > Azure Quick Deploy** dashboard in Citrix DaaS for Azure, expand **Troubleshoot & Support** on the right.
2. Click **View troubleshooting options**.
3. On the **Troubleshoot** page, select **Other catalog issue**.
4. On the **Troubleshoot with RDP Access** page, select the catalog.

   If RDP has already been enabled to the selected catalog's network connection, skip to step 7.
5. The RDP access range is displayed. If you want to restrict RDP access to a smaller range than permitted by the network connection, select the **Restrict RDP access to only computers in IP address range** check box and then enter the desired range.
6. Click **Enable RDP Access.**

   When RDP access is successfully enabled, the page title changes to **RDP Access –*connection***.

   If RDP access is not successfully enabled, click **Retry Enabling RDP** at the bottom of the failure notification page.
7. Connect to machines using your Active Directory administrator credentials. You can then collect logs and run diagnostics.

Get help

If you still have problems, open a ticket by following the instructions in How to Get Help and Support.

Limits

February 27, 2023

This article lists the limits for resources in a Citrix DaaS Standard for Azure (formerly Citrix Virtual Apps and Desktops Standard for Azure service) deployment.

> **Note:**
>
> The limits are Citrix recommended.

Configuration limits

Resource	Limit
Active Directory domains	25
Catalogs	100
Resource locations	25
VDAs per subscription	2,500

Resource location limits

The following table lists the limits for each resource location. If your requirements exceed these limits, Citrix recommends using more resource locations.

Resource	Limit
Active Directory domains	1
Single-session VDAs	10,000
Multi-session VDAs	1,000

Citrix Cloud Connectors are assigned to resource locations and link workloads to Citrix DaaS for Azure. For information about Cloud Connector limits and for size and scale recommendations, see Size and scale considerations for Cloud Connectors.

Provisioning limits

The following table lists the recommended maximums for a single Citrix Cloud account.

For larger-scale deployments, Citrix recommends a hub-and-spoke model, where VDAs are distributed across multiple subscriptions and network connections.

Resource	Limit
Multi-session VDAs per catalog	500
Single-session VDAs per catalog	1,200
VDAs per Microsoft Azure subscription	2,500

Usage limits

Resource	Limit
Concurrent Monitor full administrators	5
Concurrent end users	100,000
Resources published to a single user	250
Session launches per minute	3,000

Trial limits

The following table lists the limits during a trial of Citrix DaaS for Azure.

Azure subscription	Resource	Limit
Citrix Managed Azure subscription	Maximum number of catalogs	3
	Maximum number of users	25
	Maximum number of VDAs per catalog	3
Customer-managed Azure subscription	Maximum number of catalogs	10
	Maximum number of users	25

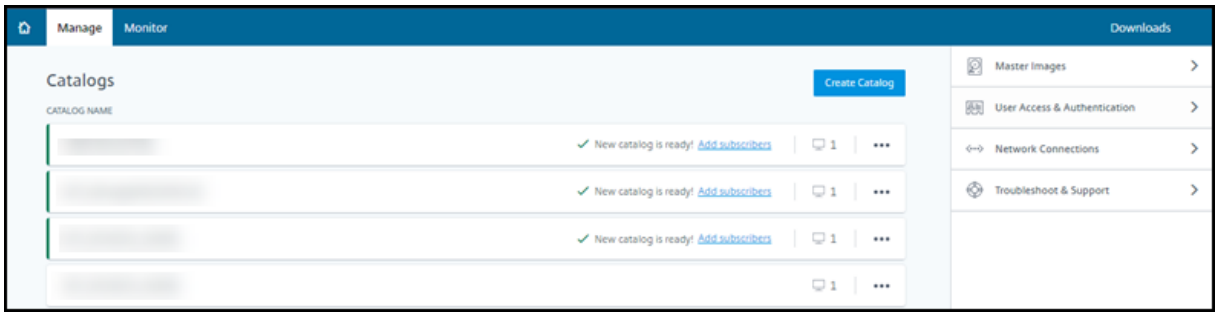
Azure subscription	Resource	Limit
	Maximum number of VDAs per catalog	10

Reference

August 30, 2022

Dashboards

Most administrator activities for Citrix DaaS Standard for Azure (formerly Citrix Virtual Apps and Desktops Standard for Azure service) can be entered through the **Manage** and **Monitor** dashboards. After you create your first catalog, the **Manage** dashboard launches automatically when you sign in to Citrix Cloud and select Citrix DaaS for Azure.



You can access the dashboards after your request for a trial or purchase is approved and completed.

To access the dashboards:

1. Sign in to Citrix Cloud.
2. In the upper left menu, select **My Services > DaaS Standard for Azure**. (Alternatively, you can click **Manage** on the **DaaS Standard for Azure** tile in the main area of the display.)
3. If a catalog has not been created yet, click **Get Started** on the **Welcome** page. You're taken to the **Manage > Azure Quick Deploy** dashboard.
4. If a catalog has already been created, you're taken automatically to the **Manage > Azure Quick Deploy** dashboard.
5. To access the **Monitor** dashboard, click the **Monitor** tab.

For in-product guidance from the dashboard, click the icon in the lower right corner.

Catalog tabs on the Manage dashboard

From the **Manage > Azure Quick Deploy** dashboard, click anywhere in the catalog's entry. The following tabs contain information about the catalog:

- **Details:** Lists the information specified when the catalog was created (or its most recent edit). It also contains information about the image that was used to create the catalog.

  From this tab, you can:

  - Change the image that is used in the catalog.
  - Delete the catalog.
  - Access the page containing details for the resource location used by the catalog.

- **Desktop:** Available only for catalogs containing single-session (static or random) machines. From this tab, you can change the name and description of the catalog.

- **Desktop and Apps:** The **Desktops and Apps** tab is available only for catalogs containing multi-session machines. From this tab, you can:

  - Add, edit, or remove applications that the catalog's users can access in Citrix Workspace.
  - Change the name and description of the catalog.

- **Subscribers:** Lists all users, including their type (user or group), account name, display name, plus their Active Directory domain and user principal name.

  From this tab, you can add or remove users for a catalog.

- **Machines:** Shows the total number of machines in the catalog, plus the number of registered machines, unregistered machines, and machines that have maintenance mode turned on.

  For each machine in the catalog, the display includes each machine's name, power state (on/off), registration state (registered/unregistered), assigned users, session count (0/1), and maintenance mode status (an icon indicating on or off).

  From this tab, you can:

  - Add or delete a machine
  - Start, restart, force restart, or shut down a machine
  - Turn a machine's maintenance mode on or off

  For details, see Manage catalogs. Many of the machine actions are also available from the **Monitor** dashboard. See Monitor and power control machines.

- **Power Management:** Enables you to manage when machines in the catalog are powered on and off. A schedule also indicates when idle machines are disconnected.

  You can configure a power schedule when you create a custom catalog or later. If no schedule is explicitly set, a machine powers off when a session ends.

  When creating a catalog using quick create, you cannot select or configure a power schedule. By default, quick create catalogs use the Cost Saver preset schedule. However, you can edit that catalog later and change the schedule.

  For details, see Manage power management schedules.

DNS servers

This section applies to all deployments that contain domain-joined machines. You can ignore this section if you use only non-domain-joined machines.

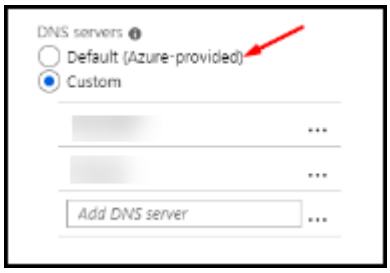
1. Before creating a domain-joined catalog (or a connection, if you're using a Citrix Managed Azure subscription), check whether you have DNS server entries that can resolve public and private domain names.

   When Citrix DaaS for Azure creates a catalog or a connection, it looks for at least one valid DNS server entry. If no valid entries are found, the creation operation fails.

   Where to check:

   - If you are using your own Azure subscription, check the **DNS servers** entry in your Azure.
   - If you are using a Citrix Managed Azure subscription and creating an Azure VNet peering connection, check the **DNS servers** entry in the Azure VNet that you're peering.
   - If you are using a Citrix Managed Azure subscription and creating an SD-WAN connection, check the DNS entries in the SD-WAN Orchestrator.

2. In Azure, the **Custom** setting must have at least one valid entry. Citrix DaaS for Azure cannot be used with the **Default (Azure-provided)** setting.

   - If **Default (Azure-provided)** is enabled, change the setting to **Custom**, and add at least one DNS server entry.

- If you already have DNS server entries under **Custom**, verify that the entries you want to use with Citrix DaaS for Azure can resolve public and private domain IP names.
- If you do not have any DNS servers that can resolve domain names, Citrix recommends adding an Azure-provided DNS server that has those capabilities.

3. If you change any DNS server entries, restart all machines that are connected to the virtual network. The restart assigns the new DNS server settings. (The VMs continue using their current DNS settings until the restart.)

If you want to change DNS addresses later, after a connection is created:

- When using your own Azure subscription, you can change them in Azure (as described in the preceding steps). Or, you can change them in Citrix DaaS for Azure.
- When using a Citrix Managed Azure subscription, Citrix DaaS for Azure does not synchronize DNS address changes that you make in Azure. However, you can change DNS settings for the connection in Citrix DaaS for Azure.

Keep in mind that changing DNS server addresses can potentially cause connectivity issues for machines in catalogs that use that connection.

Adding DNS servers through Citrix DaaS for Azure

Before adding a DNS server address to a connection, make sure that the DNS server can resolve public and internal domain names. Citrix recommends that you test connectivity to a DNS server before adding it.

1. To add, change, or remove a DNS server address when you're creating a connection, click **Edit DNS servers** on the **Add** *connection type* page. Or, if a message indicates that no DNS server addresses were found, click **Add DNS Servers**. Continue with step 3.
2. To add, change, or remove a DNS server address for an existing connection:
   a) From the **Manage > Azure Quick Deploy** dashboard, expand **Network Connections** on the right.
   b) Select the connection you want to edit.
   c) Click **Edit DNS servers**.
3. Add, change, or remove addresses.
   a) To add an address, click **Add DNS server** and then enter the IP address.
   b) To change an address, click inside the address field and change the numbers.
   c) To remove an address, click the trash icon next to the address entry. You cannot remove all DNS server addresses. The connection must have at least one.
4. When you're done, click **Confirm Changes** at the bottom of the page.

5. Restart all machines that use that connection. The restart assigns the new DNS server settings. (The VMs continue using their current DNS settings until the restart.)

Policies

Set group policies for non-domain-joined machines

1. RDP to the machine that is being used for the image.
2. Install Citrix Group Policy Management:
   a) Browse to CTX220345. Download the attachment.
   b) Double-click the downloaded file. In the `Group Policy Templates 1912 > Group Policy Management` folder, double-click `CitrixGroupPolicyManagement_x64.msi`.
3. Use the **Run** command to start `gpedit.msc`, which opens the Group Policy Editor.
4. In `User Configuration Citrix Policies > Unfiltered`, click **Edit Policy**.

   If the Group Policy Management Console fails (as described in CTX225742), install the Microsoft Visual C++ 2015 Runtime (or a later version of that runtime).
5. Enable policy settings as needed. For example:
   - When working in **Computer Configuration** or **User Configuration** (depending on what you want to configure) on the **Settings** tab, in `Category > ICA / Printing`, select **Auto-create PDF Universal Printer** and set to `Enabled`.
   - If you want logged-in users to be administrators of their desktop, add the **Interactive User** group to the built-in administrators group.
6. When you're done, save the image.
7. Either update the existing catalog or create a new catalog using the new image.

Set group policies for domain-joined machines

1. Ensure that the Group Policy Management feature is installed.
   - On a Windows multi-session machine, add the Group Policy Management feature, using the Windows tool for adding roles and features (such as **Add Roles and Features**).
   - On a Windows single-session machine, install the Remote Server Administration Tools for the appropriate OS. (This installation requires a domain admin account.) After that installation, the Group Policy Management console is available from the **Start** menu.

2. Download and install the Citrix Group Policy management package from the Citrix download page, and then configure policy settings as needed. Follow the procedure in Set group policies for non-domain-joined machines, step 2 through the end.

> **Note:**
>
> Although the Citrix Studio console is not available in Citrix DaaS for Azure, see the Policy settings reference articles to learn about what's available.

Resource location actions

Citrix automatically creates a resource location and two Cloud Connectors when you create the first catalog for publishing desktops and apps. You can specify some information related to the resource location when you create a catalog. See Resource location settings when creating a catalog.

(For Remote PC Access, you create the resource location and Cloud Connectors.)

This section describes available actions after a resource location is created.

1. From the **Manage > Azure Quick Deploy** dashboard, expand **Cloud Subscriptions** on the right.
2. Click the subscription.
   - The **Details** tab shows the number and names of catalogs and images in the subscription. It also indicates the number of machines that can deliver desktops or apps. That count does not include machines used for other purposes, such as images, Cloud Connectors, or RDS license servers
   - The **Resource Locations** tab lists each resource location. Each resource location entry includes the status and address of each Cloud Connector in the resource location.

The ellipsis menu in a resource location's entry contains the following actions.

Run Health Check

Selecting **Run Health Check** starts the connectivity check immediately. If the check fails, the Cloud Connector's state is unknown, because it is not communicating with Citrix Cloud. You might want to restart the Cloud Connector.

Restart Connectors

Citrix recommends restarting only one Cloud Connector at a time. Restarting takes the Cloud Connector offline, and disrupts user access and machine connectivity.

Select the check box for the Cloud Connector you want to restart. Click **Restart**.

Add Connectors

Adding a Cloud Connector typically takes 20 minutes to complete.

Provide the following information:

- How many Cloud Connectors to add.
- Domain service account credentials, which are used to join the Cloud Connector machines to the domain.
- Machine performance.
- Azure resource group. The default is the resource group last used by the resource location.
- Organizational Unit (OU). The default is the OU last used by the resource location.
- Whether your network requires a proxy server for internet connectivity. If you indicate **Yes**, provide the proxy server FQDN or IP address, and port number.

When you're done, click **Add Connectors**.

Delete Connectors

If a Cloud Connector cannot communicate with Citrix Cloud, and a restart does not resolve the issue, Citrix Support might recommend deleting that Cloud Connector.

Select the check box for the Cloud Connector you want to delete. Then click **Delete**. When prompted, confirm the deletion.

You can also delete an available Cloud Connector. However, if deleting that Cloud Connector would result in fewer than two available Cloud Connectors in the resource location, you're not allowed to delete the selected Cloud Connector.

Select Update Time

Citrix automatically provides software updates for the Cloud Connectors. During an update, one Cloud Connector is taken offline and updated, while other Cloud Connectors remain in service. When the first update completes, another Cloud Connector is taken offline and updated. This process continues until all Cloud Connectors in the resource location are updated. The best time to start updates is usually outside your typical business hours.

Choose the time to begin updates, or indicate that you want updates to start when an update is available. When you're done, click **Save**.

Rename

Enter the new name for the resource location. Click **Save**.

Configure Connectivity

Indicate whether users can access desktops and apps through the Citrix Gateway service, or only from within your corporate network.

Profile Management

Profile Management ensures that personal settings apply to users'virtual applications, regardless of the location of the user device.

Configuring Profile Management is optional.

You can enable Profile Management with the profile optimization service. This service provides a reliable way for managing these settings in Windows. Managing profiles ensures a consistent experience by maintaining a single profile that follows the user. It consolidates automatically and optimizes user profiles to minimize management and storage requirements. The profile optimization service requires minimal administration, support, and infrastructure. Also, profile optimization provides users with an improved logon and logoff experience.

The profile optimization service requires a file share where all the personal settings persist. You manage the file servers. We recommend setting up network connectivity to allow access to these file servers. You must specify the file share as a UNC path. The path can contain system environment variables, Active Directory user attributes, or Profile Management variables. To learn more about the format of the UNC text string, see Specify the path to the user store.

When enabling Profile Management, consider further optimizing the user's profile by configuring folder redirection to minimize the effects of the user profile size. Applying folder redirection complements the Profile Management solution. For more information, see Microsoft Folder Redirection.

Configure the Microsoft RDS License Server for Windows Server workloads

This service accesses Windows Server remote session capabilities when delivering a Windows Server workload, such as Windows 2016. This typically requires a Remote Desktop Services client access license (RDS CAL). The Windows machine where the Citrix VDA is installed must be able to contact an RDS license server to request RDS CALs. Install and activate the license server. For more information, see the Microsoft document Activate the Remote Desktop Services License Server. For proof of concept environments, you can use the grace period provided by Microsoft.

With this method, you can have this service apply the license server settings. You can configure the license server and per user mode in the RDS console on the image. You can also configure the license server using Microsoft Group Policy settings. For more information, see the Microsoft document License your RDS deployment with client access licenses (CALs).

To configure the RDS license server using Group Policy settings

1. Install a Remote Desktop Services License Server on one of the available VMs. The VM must always be available. The Citrix service workloads must be able to reach this license server.
2. Specify the license server address and per-user license mode using Microsoft Group Policy. For details, see the Microsoft document Specify the Remote Desktop Licensing Mode for an RD Session Host Server.

Windows 10 workloads require appropriate Windows 10 license activation. We recommend that you follow Microsoft documentation to activate Windows 10 workloads.

Consumption commitment usage

> **Note:**
>
> This feature is in preview.

On the **General** card in the **Manage > Azure Quick Deploy** dashboard, the **Consumption** value indicates how much consumption has been used in the current calendar month. That value includes monthly and term commitments.

When you click **General**, the **Notifications** tab includes:

- Total consumption used for the month (monthly and term).
- Number of units of monthly consumption commitment.
- Percentage of term consumption commitment.

The values and progress bars can alert you to potential or actual usage overages.

Actual data can take 24 hours to appear. Usage and billing data are considered final 72 hours after the end of a calendar month.

For more usage information, see Monitor licenses and usage for Citrix DaaS Standard for Azure.

You can optionally request notifications to appear in the **Manage** dashboard when consumption usage (for monthly, term, or both commitments) reaches a specified level. By default, notifications are disabled.

1. On the **Notifications** tab, click **Edit Notification Preferences**.
2. To enable notifications, click the slider so that the check mark appears.
3. Enter a value. Repeat for the other consumption type, if needed.
4. Click **Save**.

To disable notifications, click the slider so that the check mark no longer appears, and then click **Save**.

Monitor Citrix license usage

To view your Citrix license usage information, follow the guidance in Monitor licenses and usage for Citrix DaaS Standard for Azure. You can view:

- Licensing summary
- Usage reports
- Usage trends and license activity
- Licensed users

You can also release licenses.

Load balancing

Load balancing applies to multi-session machines, not single-session machines.

> **Important:**
>
> Changing the load balancing method affects all catalogs in your deployment. That includes all catalogs created using any supported host type, cloud-based and on-premises, regardless of interface used to create them (such as Studio or Quick Deploy).
>
> Make sure you have maximum session limits configured for all catalogs before proceeding.
>
> - In the Quick Deploy management interface for Citrix DaaS for Azure, that setting is located on each catalog's **Details** tab.
> - In other Citrix DaaS services and editions, use load management policy settings.

Load balancing measures the machine load, and determines which multi-session machine to select for an incoming user session under the current conditions. This selection is based on the configured load balancing method.

You can configure one of two load balancing methods: horizontal or vertical. The method applies to all multi-session catalogs (and therefore, all multi-session machines) in your service deployment.

- **Horizontal load balancing:** An incoming user session is assigned to the least-loaded powered-on machine available.

  Simple example: You have two machines configured for 10 sessions each. The first machine handles five concurrent sessions. The second machine handles five.

  Horizontal load balancing offers high user performance, but it can increase costs as more machines are kept powered-on and busy.

  This method is enabled by default.

- **Vertical load balancing:** An incoming user session is assigned to the powered-on machine with the highest load index. (Citrix DaaS for Azure calculates and then assigns a load index for every multi-session machine. The calculation considers factors such as CPU, memory, and concurrency.)

  This method saturates existing machines before moving on to new machines. As users disconnect and free up capacity on existing machines, new load is assigned to those machines.

  Simple example: You have two machines configured for 10 sessions each. The first machine handles the first 10 concurrent sessions. The second machine handles the eleventh session.

  With vertical load balancing, sessions maximize powered-on machine capacity, which can save machine costs.

To configure the load balancing method:

1. From the **Manage > Azure Quick Deploy** dashboard, expand **General** on the right.
2. Under **Global Settings**, click **View All**.
3. On the **Global Settings** page, under **Multi-Session Catalog Load Balancing**, choose the load balancing method.
4. Click **Confirm**.

Create a catalog in a network that uses a proxy server

Follow this procedure if your network requires a proxy server for Internet connectivity, and you are using your own Azure subscription. (Using a Citrix Managed Azure subscription with a network requiring a proxy server is not supported.)

1. From **Manage > Azure Quick Deploy** dashboard, start the catalog creation process by providing the required information and then clicking **Create Catalog** at the bottom of the page.
2. The catalog creation fails because of the proxy requirement. However, a resource location is created. That resource location's name begins with "DAS", unless you provided a resource location name when creating the catalog. In the Citrix DaaS for Azure console, expand **Cloud Subscriptions**. On the **Resource Locations** tab, check whether the newly created resource location has any Cloud Connectors in it. If it does, delete them.
3. In Azure, create two VMs (see Cloud Connector system requirements). Join those machines to the domain.
4. From the Citrix Cloud console, install a Cloud Connector on each VM. Make sure the Cloud Connectors are in the same resource location that was created earlier. Follow the guidance in:
   - Cloud Connector proxy and firewall configuration
   - System and connectivity requirements

5. From the **Manage > Azure Quick Deploy** dashboard, repeat the catalog creation process. When the catalog is created, it uses the resource location and Cloud Connectors you created in the preceding steps.

Get help

- Review Troubleshoot.
- If you need further assistance with Citrix DaaS for Azure, open a support ticket by following the guidance in How to Get Help and Support.