



Citrix Managed Desktops

Contents

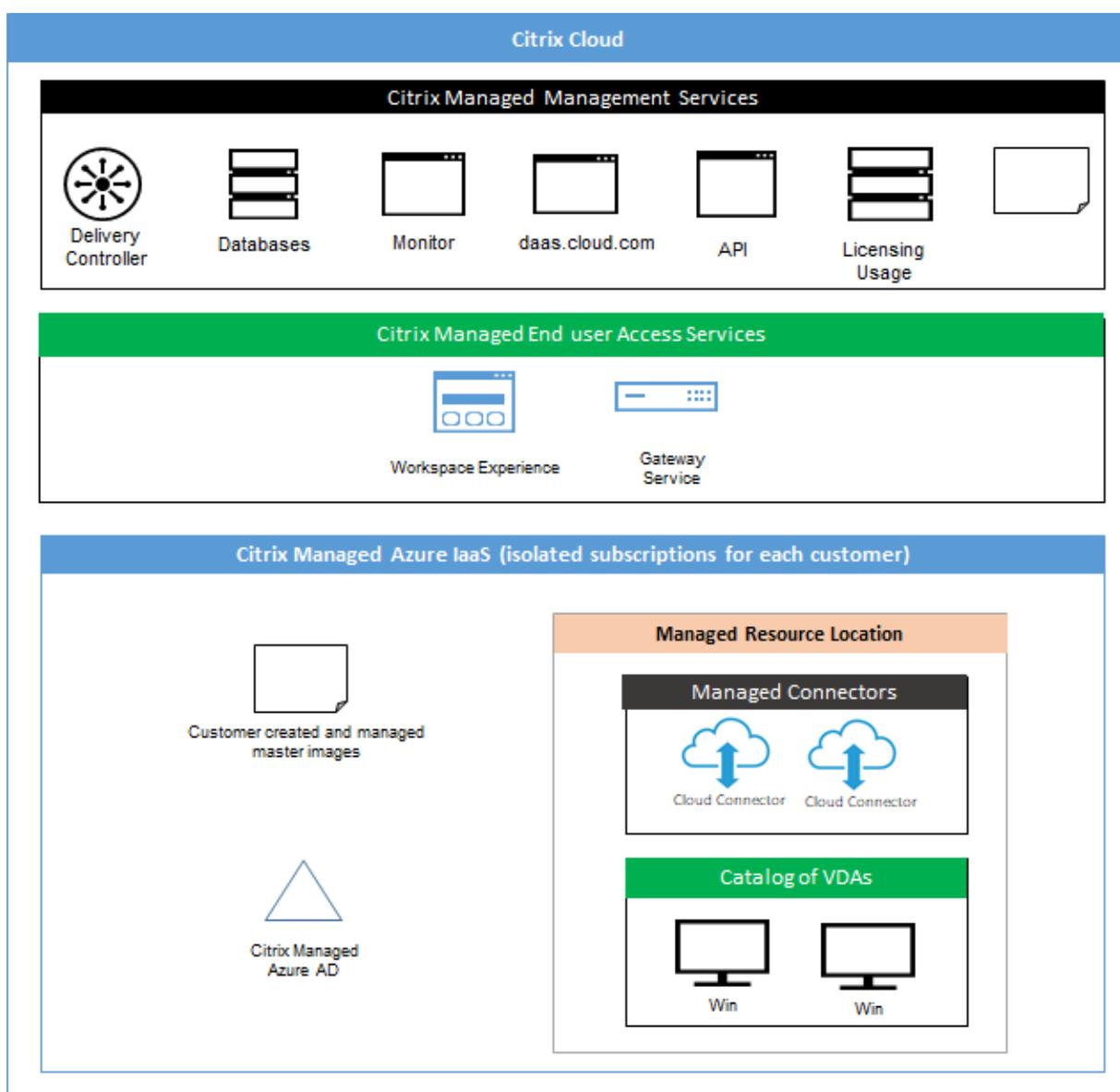
Citrix Managed Desktops	3
Technical security overview	13
Get started	26
Create catalogs	30
Azure subscriptions	38
Network connections	44
Master images	61
Users and authentication	70
Manage catalogs	76
Monitor	87
Citrix Managed Desktops service for Citrix Service Providers	93
Troubleshoot	97
Limits	102
Reference	103

Citrix Managed Desktops

June 17, 2020

Introduction

Citrix Managed Desktops is the simplest, fastest way to deliver Windows apps and desktops from Microsoft Azure. Citrix Managed Desktops 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 Windows Virtual Desktops, and apps from multi-session Windows 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-managed single-session and multi-session images that have the latest 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.

If you're familiar with Citrix Virtual Apps and Desktops, Citrix Managed Desktops significantly simplifies the deployment of virtual apps and desktops, as Citrix can manage the infrastructure for hosting those workloads.

Citrix Managed Desktops is a Citrix Cloud service. Citrix Cloud is the platform that hosts and administers Citrix services. [Learn more about Citrix Cloud](#).

To learn more about Citrix Managed Desktops components, data flow, and security considerations, see [Technical security overview](#).

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 set up a catalog of machines that deliver desktops and apps, the service displays the Citrix 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 Managed Desktops:

- Catalogs
- Master images
- Azure subscriptions

- Network connections.
- Domain-joined and non-domain-joined

Catalogs

The desktops and apps that Citrix Managed Desktops delivers to your users reside on virtual machines (VMs). Those VMs are created in a catalog.

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.

If you're familiar with other Citrix Virtual Apps and Desktops products, a catalog in this service is similar to combining a machine catalog and a delivery group. (The catalog and delivery group creation workflows in other services are not available in this service.)

Learn more about [creating](#) and [managing](#) catalogs.

Resource locations

A catalog's VMs reside in a [resource location](#). A resource location also contains two or more [Cloud Connectors](#). Citrix automatically creates the resource location and the Cloud Connectors when you create the first catalog.

When you create more catalogs, 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.

When you use your own Azure subscription, you can [add more Cloud Connectors](#) to the resource location.

Machine names

Citrix Managed Desktops uses the following default naming scheme when it creates machines.

- For Cloud Connectors, the name includes [edge](#).
- For machines that deliver desktops and apps: `DAS%-%-%-%-**-#####`

Where % = five random alpha numeric chars matching the resource location prefix, * = two random alphanumeric chars for the catalog, and ## = three digits.

Master images

When you create a catalog, a master image is used (with other settings) as a template for creating the machines.

- Citrix Managed Desktops provides several Citrix-managed master 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

The Citrix-managed master images already have a 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 the service.

- You can also import and use your own master image 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](#) is often used to refer to the machine that delivers apps or desktops, and the software component installed on that machine.

Learn more about [master images](#), and how to use them.

Azure subscriptions

You can create catalogs and build/import master images in either in a Citrix-managed Azure subscription or in your own Azure subscription.

See [Deployment scenarios](#) for information about using the Citrix-managed Azure subscription or your own.

Learn more about [Azure subscriptions](#).

Network connections

When creating a catalog, you indicate if and how users can access locations and resources on their corporate on-premises network from their Citrix Managed Desktops desktops and apps.

When using the Citrix-managed Azure subscription, 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 to Citrix Managed Desktops. You only need to add your subscription to Citrix Managed Desktops.

Learn more about [Network connections](#).

Domain-joined and non-domain-joined

Several service operations and features differ, depending on whether the machines that deliver desktops and apps are domain-joined or non-domain-joined. This 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.

The following table explains the major differences between non-domain-joined and domain-joined machines.

Non-domain-joined	Domain-joined
Do not need a connection to on-premises network.	Must have a connection to on-premises network, using Microsoft Azure VNet or Citrix SD-WAN.
Must use a Citrix-managed Azure subscription. (Cannot use your own Azure subscriptions.)	Can use a Citrix-managed Azure subscription and your own Azure subscriptions.
Active Directory is not used for machines (VDAs). VDAs are not joined to an AD domain.	Active Directory is used for machines (VDAs). VDAs are joined to an AD domain.
Active Directory group policies cannot be applied to VDAs. (You can apply local GPO on the master 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 VDA (desktop or app) launches.
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.

More technical concept information

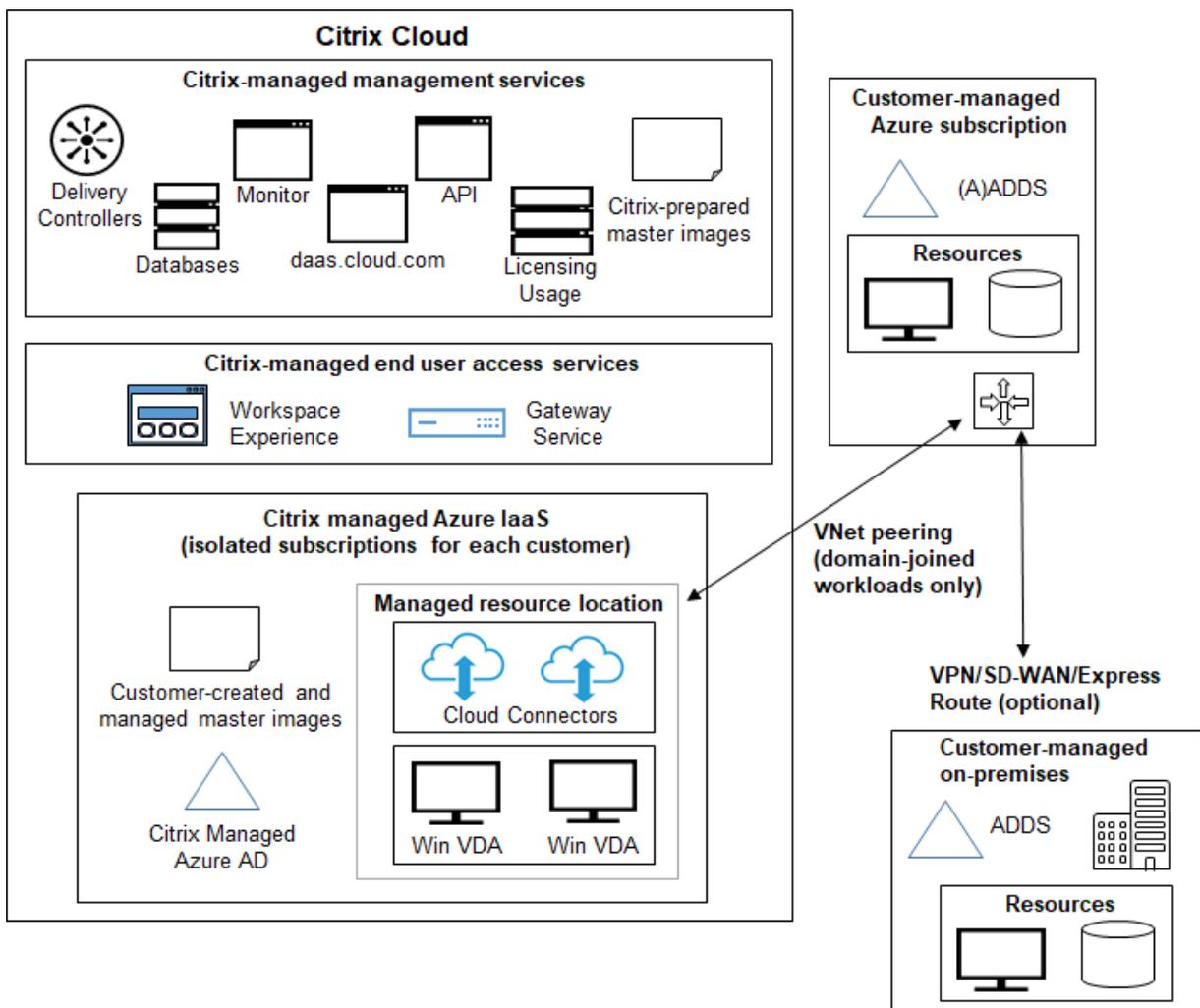
For more technical details, see the Citrix Tech Zone [reference architecture](#) and [tech brief](#).

Deployment scenarios

Deployment scenarios differ, depending on whether you're using the Citrix-managed subscription or your own customer-managed subscription.

There are differences in responsibility with Citrix-managed subscriptions and customer-managed subscriptions. For details, see [Technical security overview](#).

Deploying in the Citrix-managed subscription

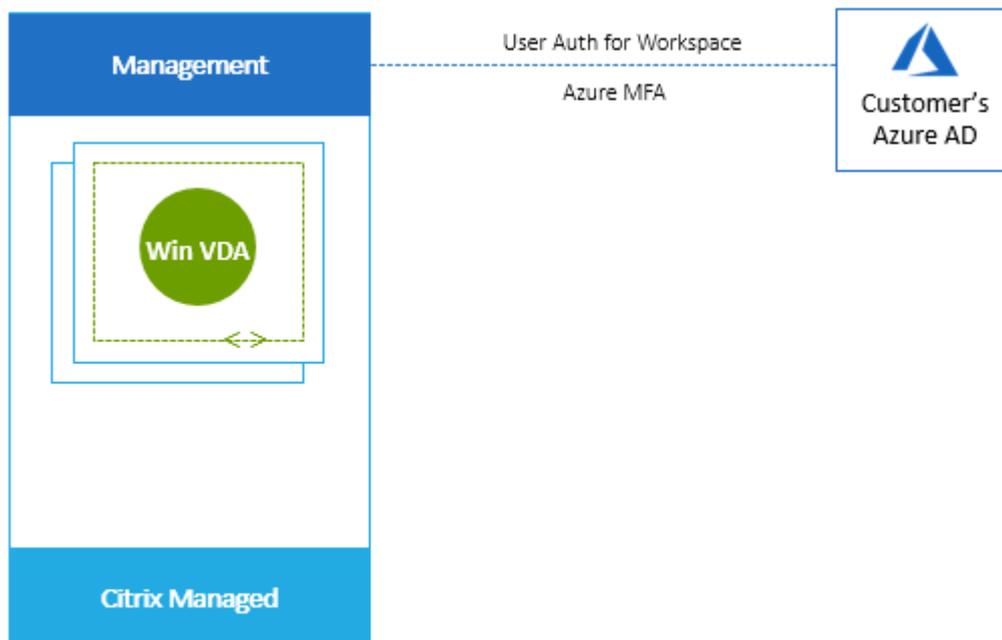


Citrix Managed Desktops supports several deployment scenarios for connection and user authentication.

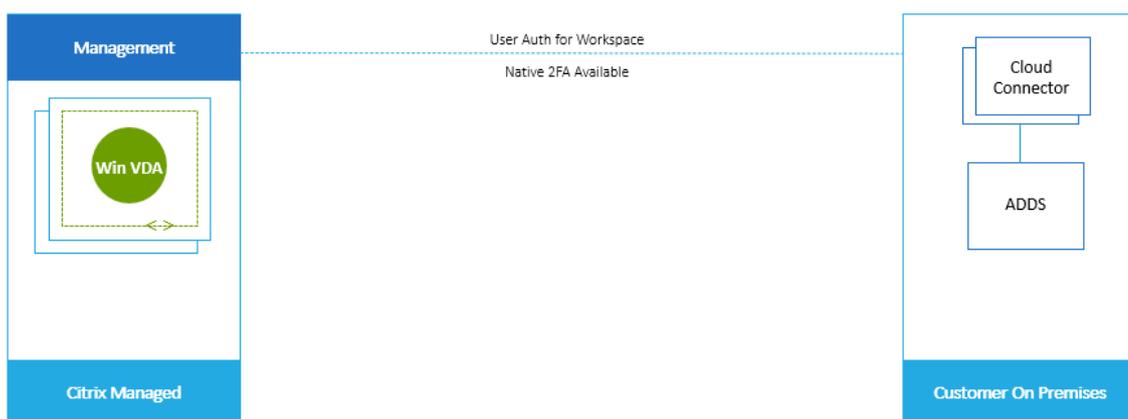
- **Managed Azure AD:** This is the simplest deployment, with non-domain-joined VDAs. It's recommended for proofs of concept. You use the Managed Azure AD to manage users. (This is a Citrix-managed Azure AD.) Your users don't need to access resources on your on-premises network.



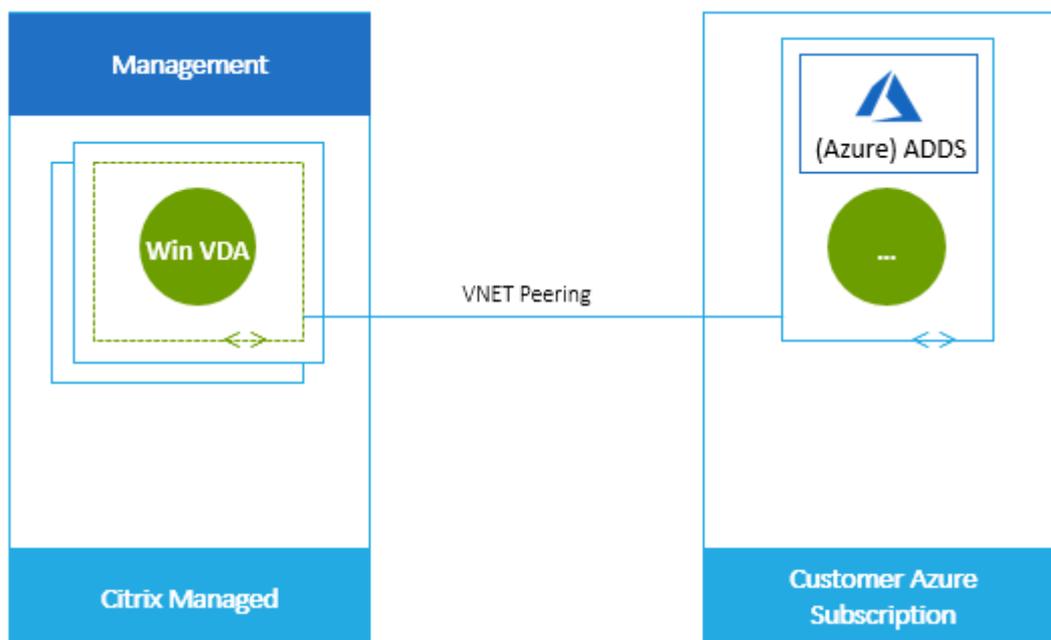
- **Customer's Azure Active Directory:** This deployment also contains non-domain-joined VDAs. You use your own Active Directory or Azure Active Directory (AAD) for end user authentication. In this scenario, your users don't need to access resources on your on-premises network.



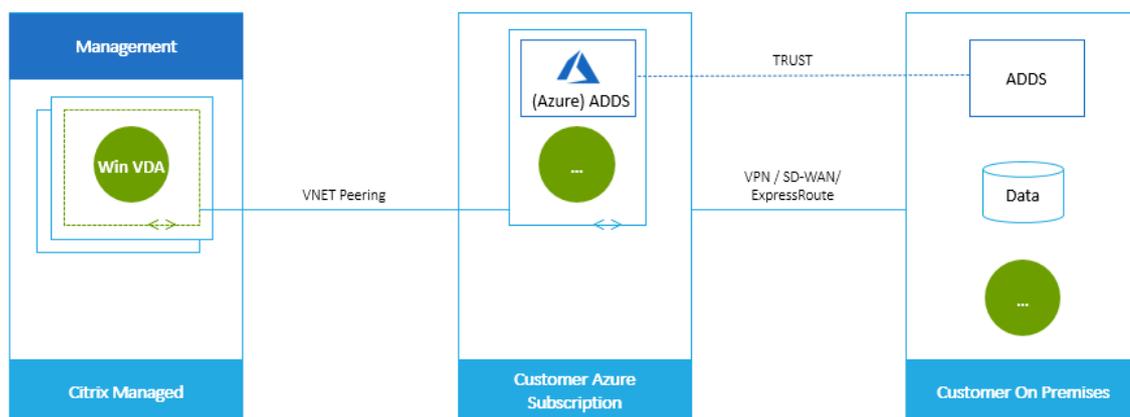
- **Customer's Azure Active Directory with on-premises access:** This deployment also contains non-domain-joined VDAs. You use your own AD or AAD for end user authentication. In this scenario, installing Citrix Cloud Connectors in your on-premises network enables access to resources in that network.



- Customer’s Azure Active Directory Domain Services and VNet peering:** If your AD or AAD resides in your own Azure VNet and 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.



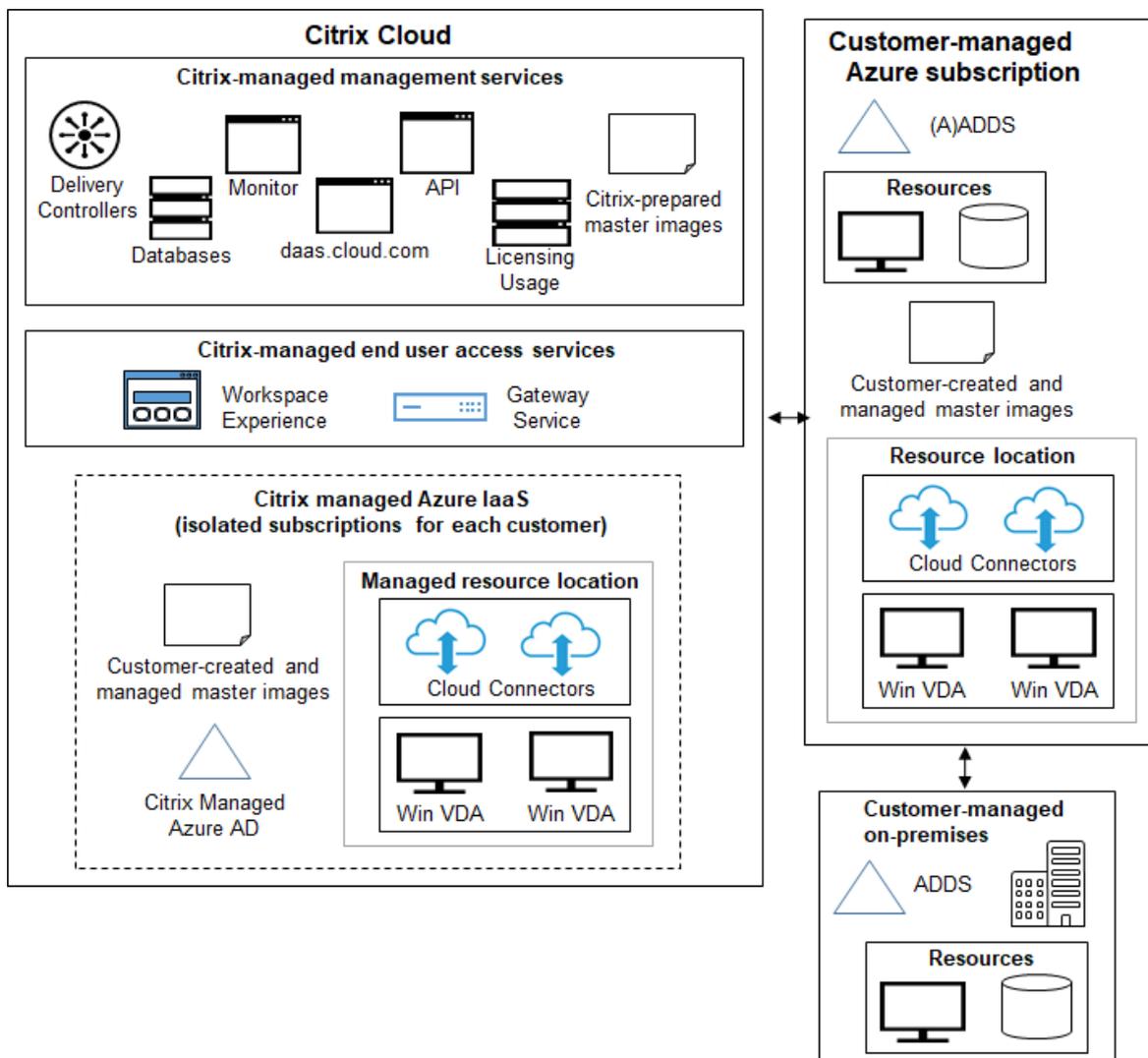
To enable your users to access data stored in your on-premises network, you can use your VPN connection from your Azure subscription to the on-premises location. Azure VNet peering is still used for network connectivity. Active Directory Domain Services in the on-premises location is used for end user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



- **Customer's Active Directory and SD-WAN:** You can provide Citrix Managed Desktops 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 Managed Desktops. Working in concert with the HDX technologies, Citrix SD-WAN provides quality-of-service and connection reliability for ICA and out-of-band Citrix Managed Desktops traffic.

Deploying in a customer-managed subscription



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

What's new

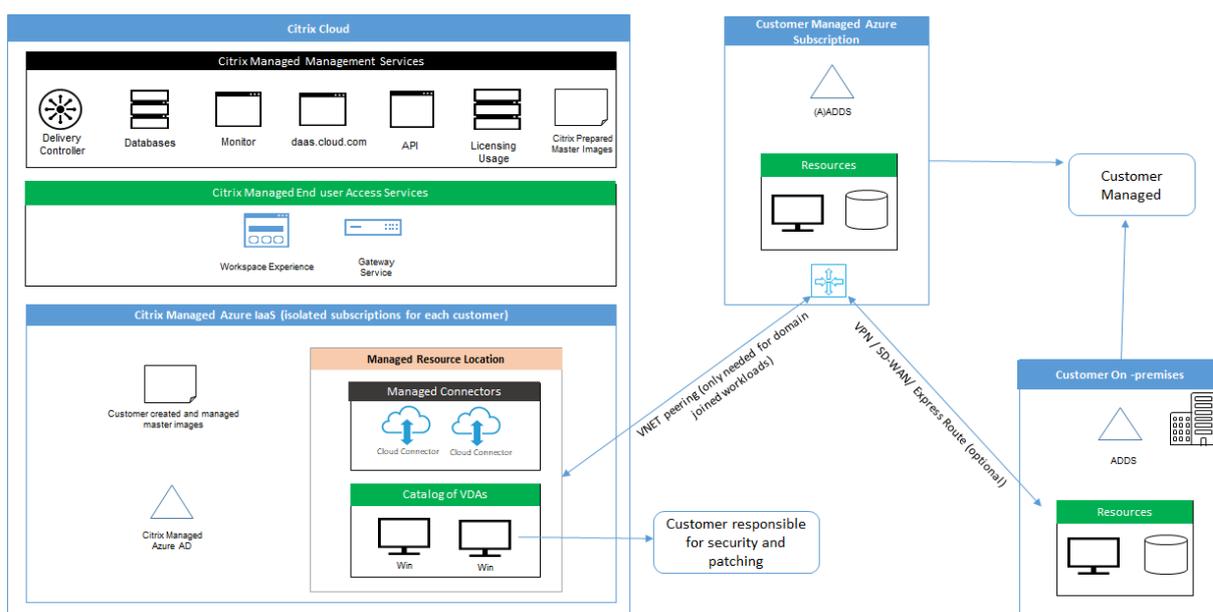
- June 2020: The [limit](#) of VDAs per subscription is now 1,200.
- May 2020: You can [add another Citrix-managed Azure subscription](#) when you need more machines than the limit per subscription.
- May 2020: Expanded information about [DNS servers](#).
- March 2020: Production support for [SD-WAN connections](#).

- February 2020: To view your Citrix license usage information, follow the guidance in [Monitor licenses and active usage for Citrix Managed Desktops service](#).
- February 2020: 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 master image containing a Citrix Linux VDA.
- February 2020: 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 is a global selection that applies to all catalogs in your deployment. See [Load balancing](#).
- February 2020: You can now add an Azure subscription if you're not a Global Admin.
- February 2020: A Citrix-managed master 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.
- January 2020: 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.
- October 2019: Added Windows Server 2012 R2 to the [Citrix-managed master images](#) list.
- October 2019: Added resource location settings information. For details, see [Resource location actions from the Manage dashboard](#) and [Resource location settings when creating a catalog](#).
- September 2019: By default, machines are created in the Citrix-managed Azure subscription. Now you can also create catalogs and images in your own customer-managed Azure subscription.

Technical security overview

May 20, 2020

The following diagram shows the components in a Citrix Managed Desktops deployment. This example uses a VNet peering connection.



With Citrix Managed Desktops, 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.

Citrix responsibility

Citrix Cloud Connectors for non-domain-joined catalogs

Citrix Managed Desktops 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 Managed Desktops service 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 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 Managed Desktops to create and customize a new master image, ports 3389-3390 are opened temporarily in the Citrix-managed VNet, so that the customer can RDP to the machine containing the new master image, to customize it.

Citrix responsibility when using VNet peering connections

For VDAs in Citrix Managed Desktops to contact on-premises domain controllers, file shares, or other intranet resources, Citrix Managed Desktops 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 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 [CTX101810](#).
 - 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 [CTX101810](#).
 - 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

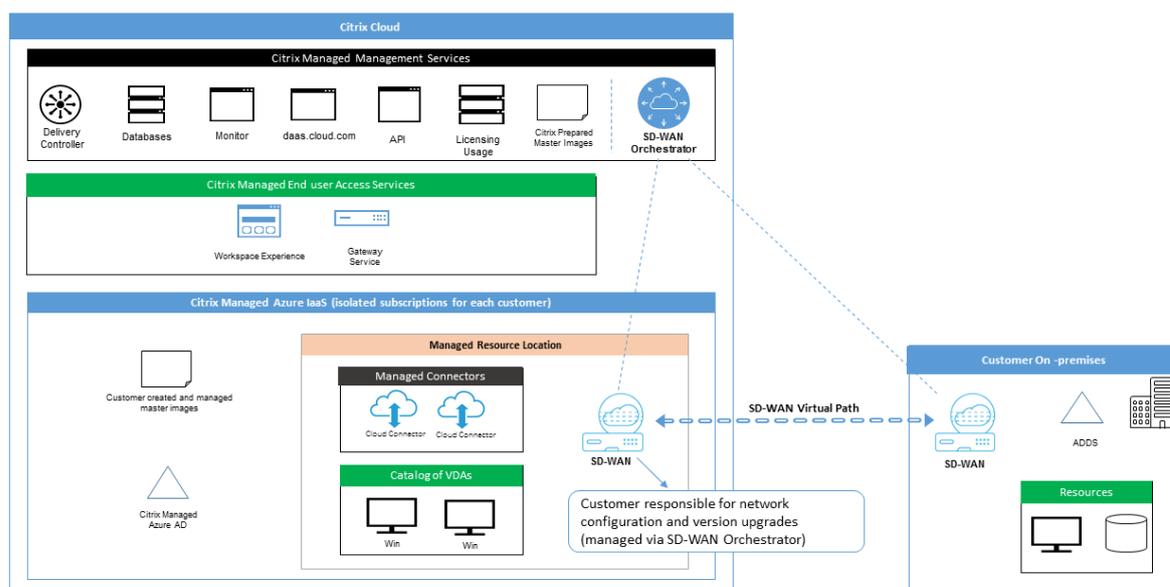
Citrix supports a fully automated way of deploying virtual Citrix SD-WAN instances to enable connectivity between Citrix Managed Desktops and on-premises resources. Citrix SD-WAN connectivity has a number of advantages compared to VNet peering, including:

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 Managed Desktops to use SD-WAN Orchestrator for managing their Citrix SD-WAN networks.

The following diagram shows the added components in a Citrix Managed Desktops deployment using SD-WAN connectivity.



The Citrix SD-WAN deployment for Citrix Managed Desktops 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 Citrix-managed 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 Managed Desktops, 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 master images

Citrix is responsible for backing up any master images uploaded to Citrix Managed Desktops, 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:

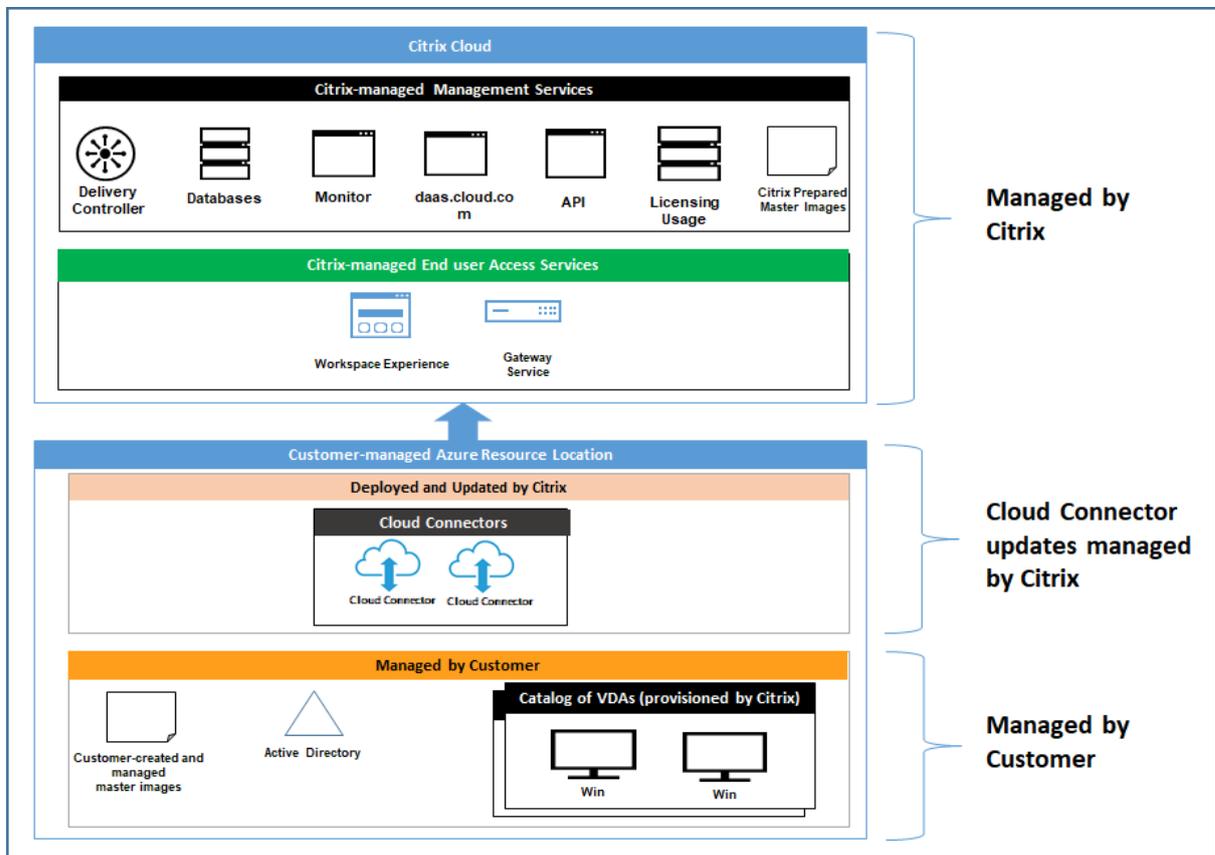
- Temporarily allow 3389 inbound from the customer-specified IP range to the bastion.
- Temporarily allow 3389 inbound from the bastion IP address to any address in the VNet (VDAs and Cloud Connectors).
- Continue to block RDP access between the Cloud Connectors, VDAs, and other VDAs.

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 master 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 master 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 Managed Desktops 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 CMD 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 Managed Desktops, 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 master 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 master 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 Managed Desktops.

Citrix and customer shared responsibilities

Citrix Cloud Connector for domain-joined catalogs

Citrix Managed Desktops 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 Managed Desktops, 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 whitelist IP ranges, 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 Managed Desktops.

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 Managed Desktops 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 Managed Desktops 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 Virtual Apps and Desktops service
- [Third party notifications](#)

Get started

May 28, 2020

This article summarizes the setup tasks for Citrix Managed Desktops. We recommend that you review each procedure's documentation before actually doing it, so you know what to expect.

Setup task summary

Links in the following sections of this article guide you through setup tasks:

1. Prepare for setup.
2. Set up a deployment, by 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, master images, network connections, or Azure subscriptions, review the introductory [concepts and terminology](#) information.

More information is available in the following articles:

- [Create catalogs](#)
 - [Master images](#)
 - [Network connections](#)
 - [Azure subscriptions](#)
 - [Users and authentication](#)
- 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 Citrix Managed Desktops service.

- Review the system requirements.
- Read through the setup steps below (proof of concept or production) to learn more.

Set up a quick proof of concept deployment

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. [Create or import a master image](#). Although you can use one of the Citrix-managed images as-is in a catalog, they're intended primarily for proof of concept deployments.
4. If you're using the Citrix-managed subscription, and want your users to be able to access items in your on-premises or other network (such as file servers), set up an [Azure VNet peering connection](#) or a [Citrix SD-WAN connection](#).
5. [Create a catalog using custom create](#).
6. If you're creating a multi-session catalog, [add apps to the catalog](#).
7. If you're using Managed Azure AD to authenticate your users, [add users to the directory](#).
8. [Add users to the catalog](#).
9. Notify your users of the Workspace URL.

After you set up the deployment, you can monitor [desktop usage](#), [sessions](#), and [machines](#).

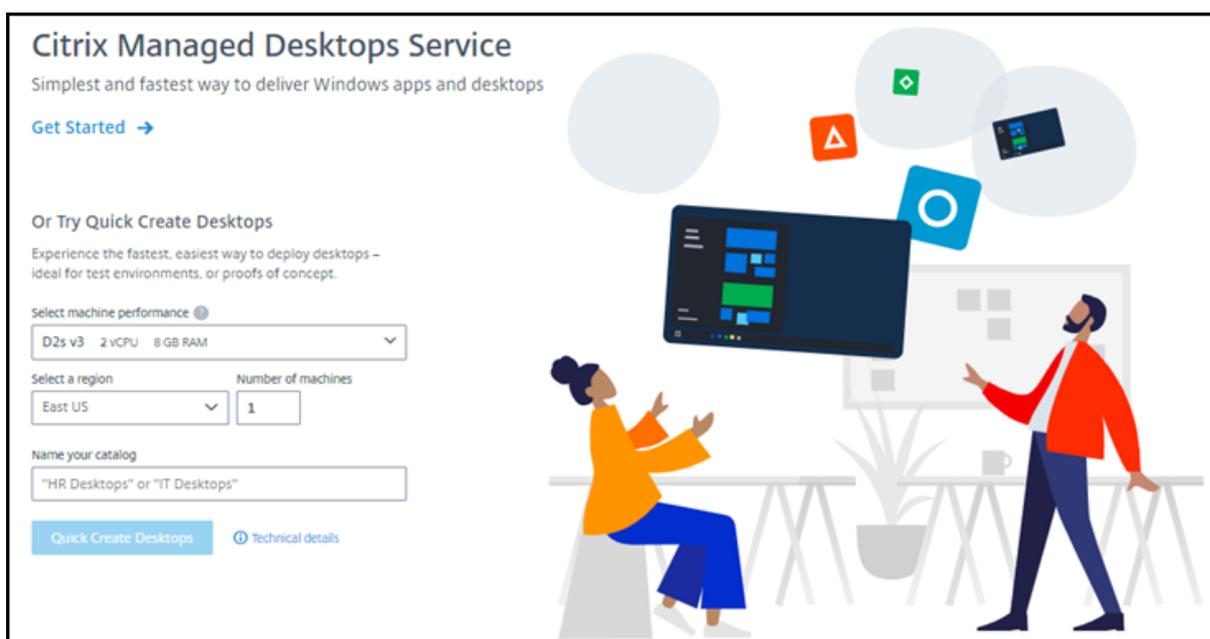
Get a Citrix Cloud account and sign up for the service

When you evaluate or purchase the Citrix Managed Desktops service, the Citrix Service Operations team provides ongoing onboarding help. That team also communicates with you to ensure that the service is running and configured correctly.

1. To sign up for a Citrix account and request a trial, go to <https://onboarding.cloud.com>. For details about that process, see [Sign up for Citrix Cloud](#).
2. After you sign in to Citrix Cloud, click **Request Trial** on the **Citrix Managed Desktops** service tile. The text changes to **Trial Requested**.

If you already subscribe to one of the Citrix Virtual Apps and Desktops services, the **Citrix Managed Desktops** tile indicates **How to Buy**. Either use a different OrgID for the Citrix Managed Desktops subscription, or decommission the Virtual Apps and Desktops service.

3. You'll receive an email when the service is available for you. Sign in to [Citrix Cloud](#).
4. On the **Managed Desktops** tile, click **Manage**. The first time you access the service, you're taken to the service's **Welcome** page.



What to do next: Continue following the setup tasks.

Other service tiles

When you receive an entitlement (as a trial or purchase) to Citrix Managed Desktops, several tiles appear on the Citrix Cloud landing page:

- Managed Desktops
- Virtual Apps and Desktops
- Gateway
- Smart Tools

Managed Desktops is the only service that is activated for your use.

If you currently subscribe to a different Citrix Virtual Apps and Desktops service

Your Citrix Cloud account allows you to subscribe to only one of the Citrix Virtual Apps and Desktops services at a time. For example, you can subscribe to Citrix Virtual Apps and Desktops OR Citrix Man-

aged Desktops, but not both. If you currently subscribe to a service, and want to subscribe to this service, you must either:

- Subscribe to this service using a different Citrix Cloud account.
- Decommission the service you already have.

For guidance, see [CTX239027](#).

Related information

[Cancel a monthly Citrix Managed Desktops subscription](#)

System requirements

For all deployments:

- **Citrix Cloud:** The Citrix Managed Desktops 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 and sign up for the service](#).
- **Windows licensing:** Ensure that you are properly licensed for Remote Desktop Services to run either Windows Server workloads or Windows Virtual Desktop Licensing for Windows 10.

If you're using the Citrix-managed subscription:

- **Azure subscriptions when using Azure VNet peering (optional):** If you plan to access resources (such as Active Directory and other file shares) in your own Azure network using Azure VNet peer connections, you must have an Azure Resource Manager 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.

- For any connection (Azure VNet peering or SD-WAN), see [Requirements for all connections](#).
- For Azure VNet peering connections, see [VNet peering requirements and preparation](#).
- For SD-WAN connections, see [SD-WAN connection requirements and preparation](#).

If you're using your own customer-managed Azure subscription, you must have an Azure Resource Manager subscription.

For Internet connectivity requirements, see [System and connectivity requirements](#).

Supported operating systems

When using the 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

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
- (Preview) Red Hat Enterprise Linux and Ubuntu

Workspace URL

After you set up the Citrix Managed Desktops environment, 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 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 Citrix Managed Desktops, open a ticket by following the instructions in [How to Get Help and Support](#).

Create catalogs

May 29, 2020

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.

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 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 combination 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.

The static and random types are sometimes called “desktop types.”

To learn about catalog information that’s displayed from the **Manage** dashboard, see [Catalog tabs on the Manage dashboard](#).

Ways to create a catalog

There are two ways to create and configure a catalog:

- **Quick create** is the fastest way to get started. You provide minimal information, and the service 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.

Here’s a comparison:

Quick create	Custom create
Less information to provide.	More information to provide.

Quick create	Custom create
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 or Azure VNet peering.
Uses a Citrix-managed Windows 10 master image. That image contains a current desktop VDA.	Choice of: Citrix-provided images, a version of a Citrix image that you've customized, or an image you imported from Azure.
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 later.)	A power management schedule can be configured during creation.
Must use the Citrix-managed subscription.	Can use the Citrix-managed or your own Azure subscription.

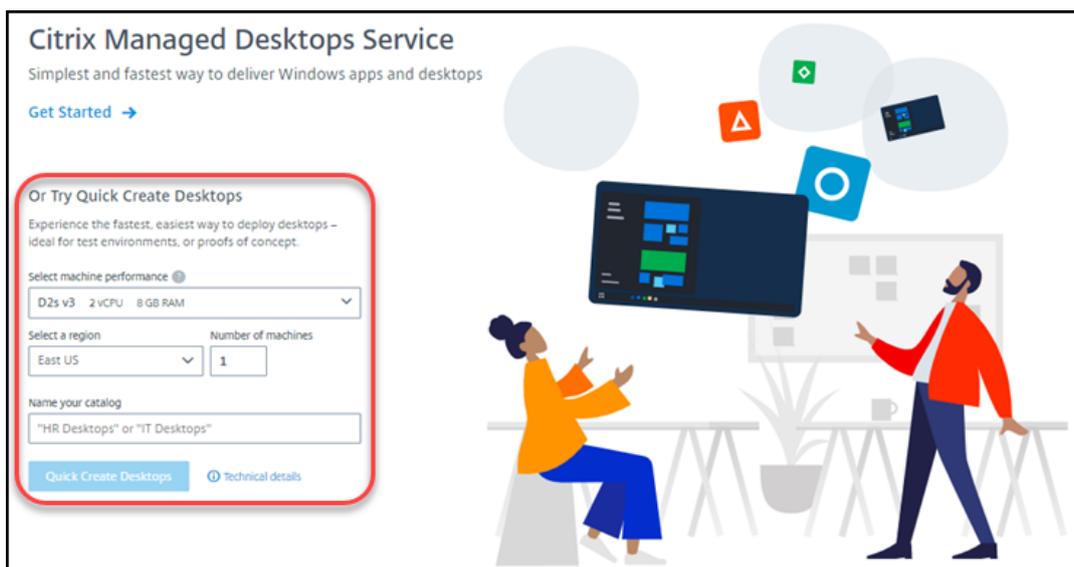
For details, see:

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

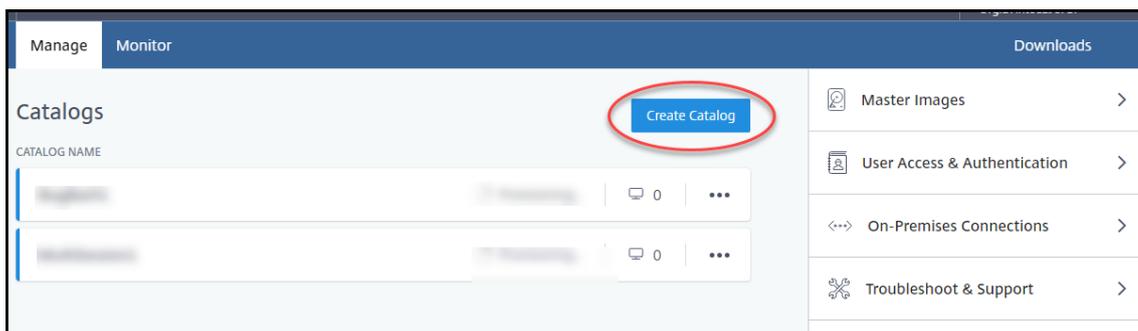
Create a catalog using quick create

This catalog creation method always uses the Citrix-managed subscription.

1. Sign in to [Citrix Cloud](#).
2. In the upper left menu, select **My Services > Managed Desktops**.
3. If a catalog has not yet been created, you're taken to the **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** dashboard. Click **Create Catalog**.
4. If a catalog has already been created (and you're creating another one), you're taken to the **Manage** dashboard. Click **Create Catalog**.



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

Create Catalog

Custom Create **Quick Create**

Select machine performance 

D2s v3 2 vCPU 8 GB RAM

Select a region

East US

Name your catalog
Enter a friendly name to identify this group of desktops like "Marketing" or "HR"

"HR Desktops" or "IT Desktops"

Number of machines

1

Quick Create Catalogs Use

- Static machines
- Managed Azure AD
- No connectivity to your corporate network
- Citrix-managed Windows 10 master image
- Cost Saver preset power settings

Create Catalog Cancel Users will be assigned after the machines

- **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 **Welcome** page, click **Quick Create Desktops**.)

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

Citrix Managed Desktops also automatically creates a resource location and adds two Cloud Connectors.

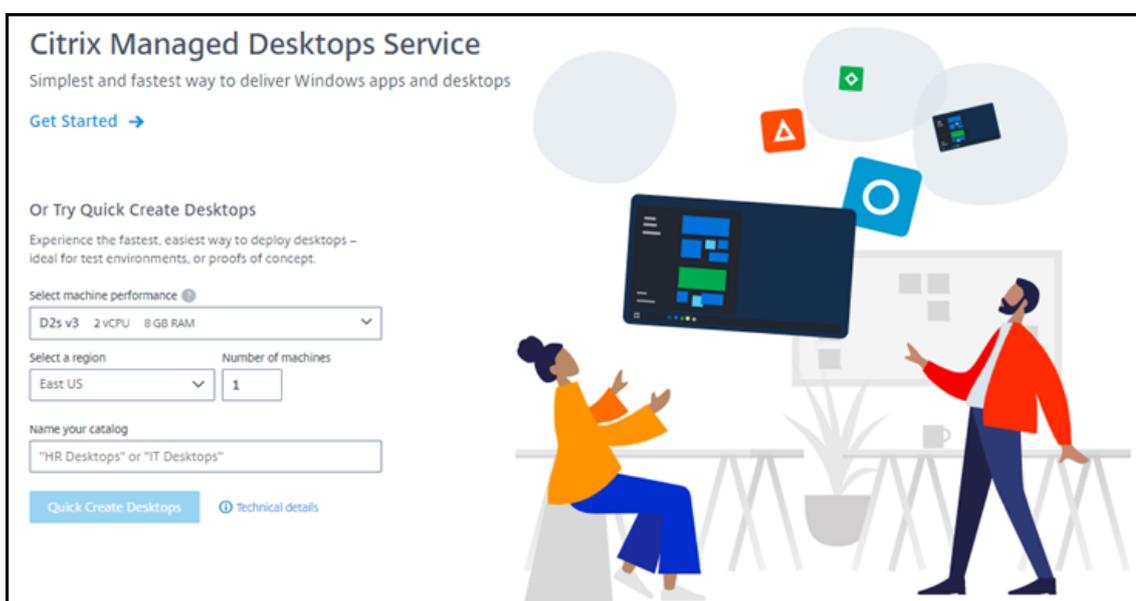
What to do next:

- If you're using 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](#).

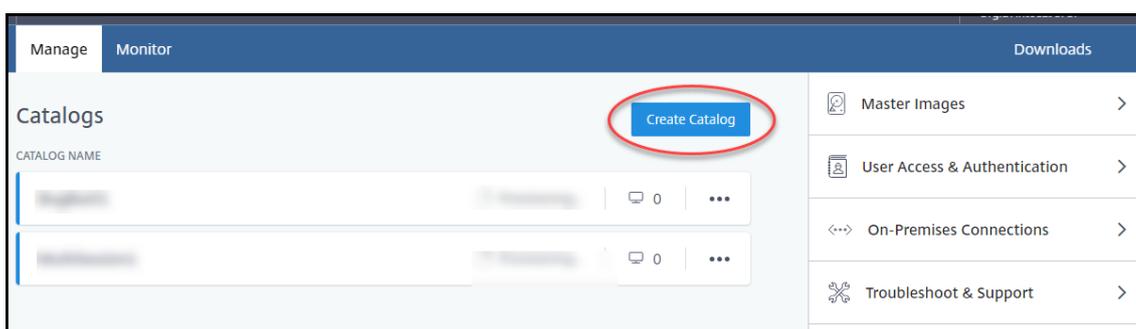
Create a catalog using custom create

If you 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.

1. Sign in to [Citrix Cloud](#).
2. In the upper left menu, select **My Services > Managed Desktops**.
3. If a catalog has not yet been created, you're taken to the **Welcome** page. Click **Get Started**. At the end of the introduction page, you're taken to the **Manage** dashboard. Click **Create Catalog**.



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



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

The screenshot shows the 'Custom Create' configuration page for Citrix Managed Desktops. The page is divided into several sections:

- Select a machine type:** Radio buttons for Multi-session (selected), Static (personal desktops), and Random (pooled desktops).
- Choose subscription:** A dropdown menu showing 'Citrix Managed'.
- Select a network connection:** A dropdown menu showing 'No connectivity to corporate network'.
- Select a region:** A dropdown menu showing 'East US'.
- Select a machine:**
 - Storage type:** A dropdown menu showing 'Standard disks (HDD)'.
 - Work Load:** A dropdown menu showing 'Light 16 sessions (D2s v3, 2 vCPU, 8 GB RAM)'.
 - Machines table:**

Machines	Sessions per machine	Total sessions
1	10	10
- Select a master image:** A dropdown menu showing 'Win 2016 Server - VDA 1906.2'.
- Name your catalog:** A text input field containing '"HR Desktops" or "IT Desktops"'. Below it is a note: 'Enter a friendly name to identify this group of desktops like "Marketing" or "HR"'. Below the input field is a link: 'Set a power schedule'.

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

- **Machine type.** For details, see Machine types.
- **Subscription.** For details, see [Azure subscriptions](#).
- **Network connection:** Select the connection to use for accessing resources in your network. For details, see [Network connections](#).

For the Citrix-managed 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 the customer-managed Azure subscription, select the appropriate resource group, virtual network, and subnet.

- **Region:** (Available only for **No Connectivity** network connection. If you selected a network connection, the catalog uses that network's region.) Select a region where you want the desktops created. You might select a region that's close to your users.
- **Machine:**

- **Storage type.** HDD or SSD.
- **Machine performance** (for **Static** or **Random** machine type), or **Workload** (for multi-session machine type).

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

- **Machine.** How many machines you want in this catalog.
- **Master image:** Select an operating system image. For details, see [Master images](#).
- **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](#).
- **Join the local Active Directory domain:** (Available only for a VNet peering network connection.) Select **Yes** or **No**. If you select **Yes**, enter the:
 - FQDN of the domain (for example, Contoso.com).
 - Organization Unit: To use the default OU (Computers), leave this field empty.
 - Service account name: Must be a domain or enterprise administrator in the format name@domain or name\domain.
 - Password for the service account name.

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

Note:

For information about *Advanced settings*, see Resource location settings when creating a catalog.

The **Manage** dashboard indicates when your catalog is created. Citrix Managed Desktops also automatically creates a resource location and adds two Cloud Connectors.

What to do next:

1. [Configure the authentication method](#) for your users to authenticate to Citrix Workspace.
2. After the catalog is created, [add users to the catalog](#).
3. If you created a multi-session catalog, [add applications](#) (before or after adding users).

Resource location settings when creating a catalog

When creating a catalog, Citrix manages the resource location for the catalog. You can optionally configure advanced settings for the resource location.

When you click **Advanced settings**, Citrix Managed Desktops retrieves resource location information.

- If you already have a resource location for the domain and network connection specified 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 specified 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.
- The OU for the resource location. By default, the OU specified for the catalog is used.
- Whether your network requires a proxy server for internet connectivity. If it does, enter the proxy server's FQDN or IP address, including the port number.
- Choose the external connectivity type: through the Citrix Gateway service, or from within your corporate network.

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

Related information

Learn about [domain-joined and non-domain-joined](#).

Azure subscriptions

May 28, 2020

Introduction

You can create catalogs and build or import master images in either in a Citrix-managed Azure subscription or your own Azure subscription.

- To use your own Azure subscriptions, you first add one or more of your Azure subscriptions to Citrix Managed Desktops. That action enables Citrix Managed Desktops to access the subscription.

Then, when you create a catalog or build/import a master image, choose the subscription you want to use. You can choose one of the subscriptions you added or a Citrix-managed subscription.

- Using a Citrix-managed subscription requires no subscription configuration. A Citrix-managed subscription is always available for catalog creation. If you haven't added any of your own Azure subscriptions to Citrix Managed Desktops, the Citrix-managed subscription is used automatically. (In other words, you don't have to select a subscription.)

If you've added your own Azure subscriptions to Citrix Managed Desktops, the Citrix-managed subscription is always a choice.

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

Citrix-managed 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 master images.	Must add the Azure subscription to Citrix Managed Desktops 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 Managed Desktops.	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 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** dashboard, 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 Managed Desktops before creating a catalog or master image that uses that subscription. You have two options when adding Azure subscriptions:

- **If you are both a Global Administrator for the directory and Owner privileges for the subscription:** Simply authenticate to your Azure account.
- **If you are not a Global Administrator and Owner on the subscription:** Before adding the subscription to Citrix Managed Desktops, 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 Managed Desktops, you provide relevant app information.

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

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

1. From the **Manage** dashboard, expand **Cloud Subscriptions** on the right.
2. Click **Add Azure subscription**.
3. On the **Add Subscriptions** page, click **Add your Azure subscription**.
4. Select **Allow Citrix Managed Desktops to access my Azure subscriptions on my 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 Managed Desktops. 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.

After the subscription addition completes, the Azure subscriptions you selected are listed when you expand **Subscriptions**. Added subscriptions are available for selection when creating a catalog or master image.

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

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

- Before you add a subscription to Citrix Managed Desktops, create an app in Azure AD and then add that app as a contributor of the subscription.
- Add the subscription to Citrix Managed Desktops, 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 Managed Desktops.
 - 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 Managed Desktops.
 - g) Select the Azure subscription you want to link to Citrix Managed Desktops, 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 Managed Desktops

You'll need the application ID, directory ID, and client secret value from the app you created in Azure AD.

1. From the **Manage** dashboard in Citrix Managed Desktops, 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 Managed Desktops dashboard, you can update the client secret or replace the Azure app from the ellipsis menu.

Add Citrix-managed Azure subscriptions

Every deployment includes a Citrix-managed Azure subscription. A Citrix-managed Azure subscription supports up to 1,000 machines. (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, such as Cloud Connectors, in a resource location.)

If your 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 subscription would exceed 1,000.

For example:

- Let's say you have two catalogs (**Cat1** and **Cat2**). Both catalogs use the same Citrix-managed 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 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 create a catalog with 75 machines (or add 75 machines to an existing catalog), using that subscription. That would exceed the subscription limit. Instead, you request another Citrix-managed subscription. Then, you 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 subscriptions (and any customer-managed Azure subscriptions that you've added) when:
 - Creating a catalog.
 - Building or importing a master image.
 - Creating a VNet peering or SD-WAN connection.

Requirement:

- You must have enough Citrix licenses to warrant adding another Citrix-managed subscription. For example, if you have 1200 Citrix licenses, in anticipation of deploying at least 1100 machines through Citrix-managed subscriptions, you can add another Citrix-managed 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** dashboard, 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 subscriptions

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

You cannot remove all Citrix-managed Azure subscriptions. At least one must remain.

1. From the **Manage** dashboard, 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 Managed Desktops. Confirm the deletion in the check boxes and then click **Yes, Delete Subscription**.

Network connections

May 1, 2020

Introduction

This article provides details about some [deployment scenarios](#) when using the Citrix-managed subscription.

When creating a catalog, you indicate if and how users access locations and resources on their corporate on-premises network from their Citrix Managed Desktops desktops and apps.

When using the Citrix-managed subscription, the choices are:

- No connectivity
- Azure VNet peering
- SD-WAN

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

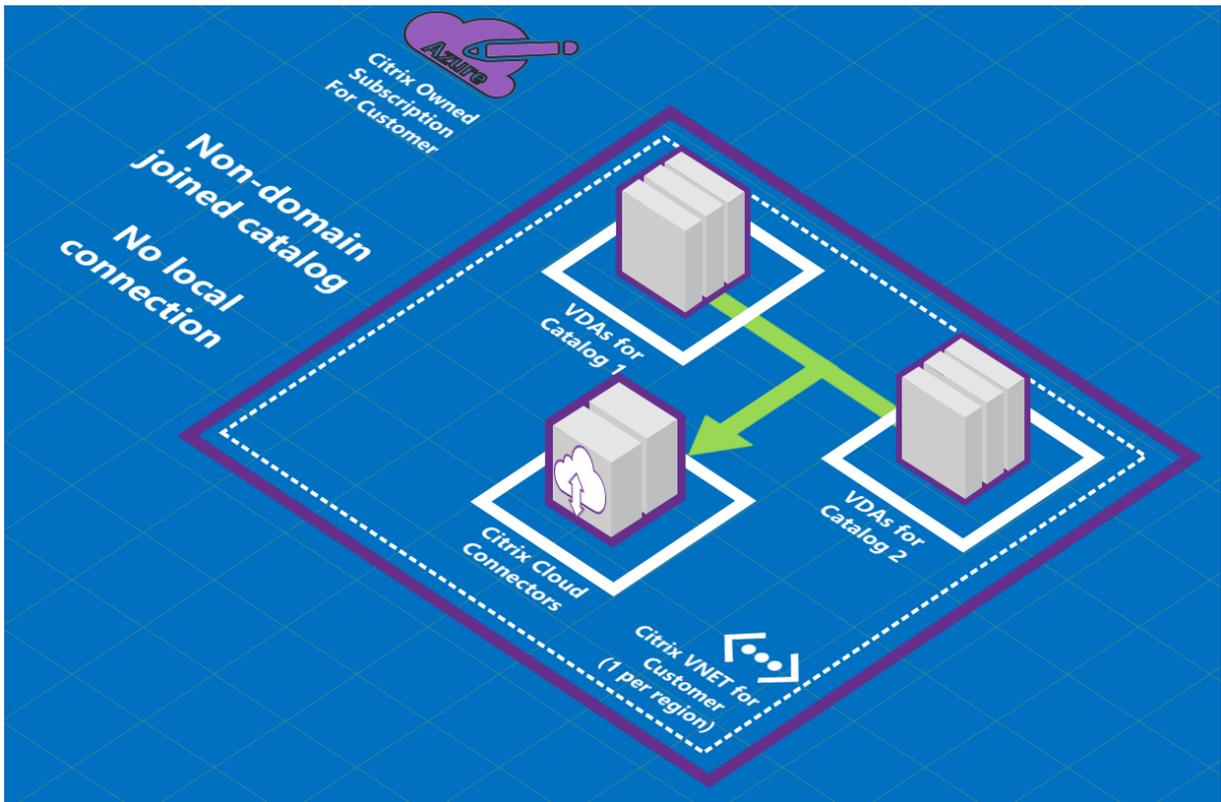
You cannot change a catalog's connection type after the catalog is created.

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 you allocated for use by Citrix Managed Desktops (specified when you create the connection) to the DNS provider's whitelisted IP addresses.
- All Citrix Managed Desktops resources that use the connection (domain-joined machines) must be able to reach your NTP server, to ensure time synchronization.

No connectivity

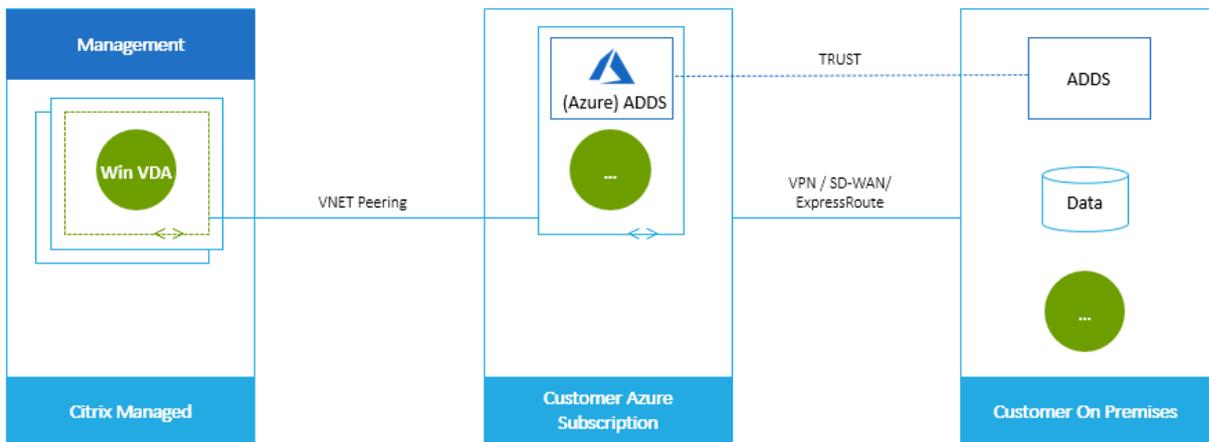
When a catalog is configured with **No connectivity**, users cannot access resources on their on-premises or other networks. This is the only choice when creating a catalog using quick create.



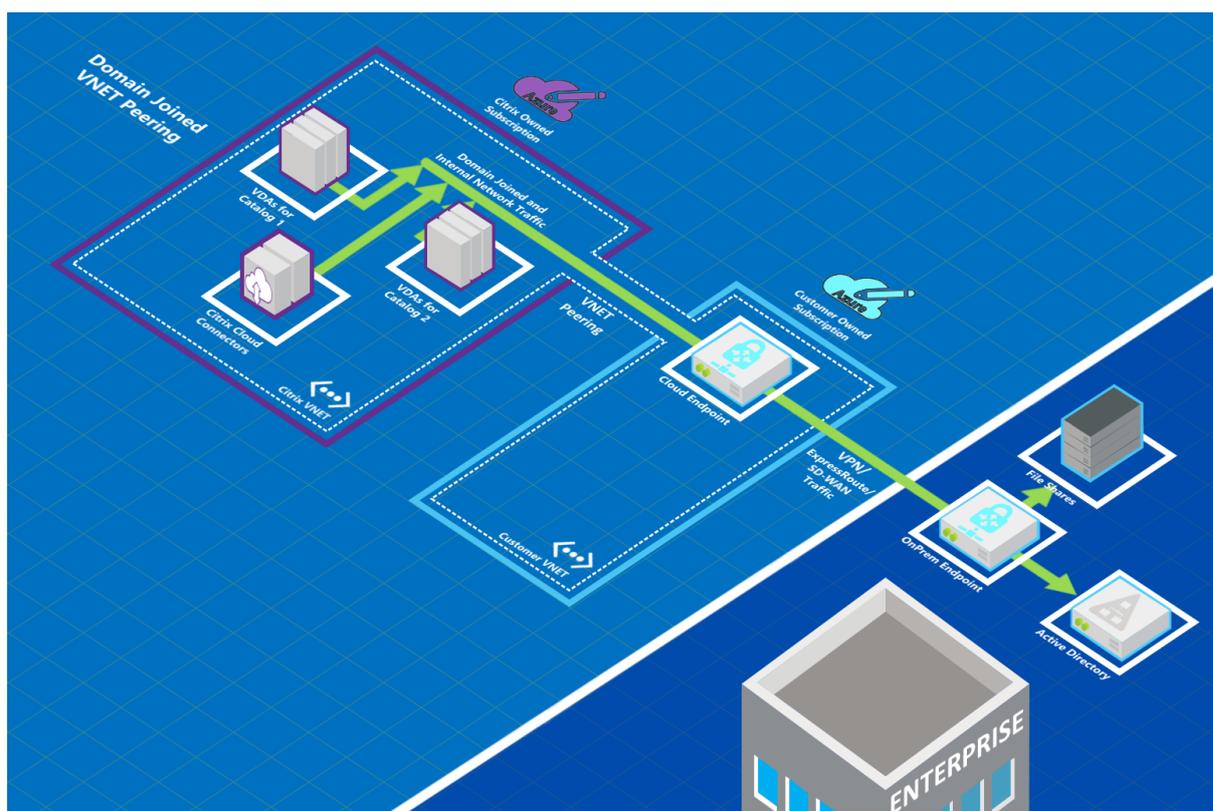
About Azure VNet peering connections

Virtual network peering seamlessly connects two Azure virtual networks (VNETs): yours and the Citrix Managed Desktops 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 in a Citrix Managed Desktops deployment.



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 Managed Desktops.
- 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 choose to use custom routes if there are networks that Managed Desktops 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 Managed Desktops environment.

- When you add custom routes, you must update your company's route tables with the Managed Desktops destination VNet information to ensure end-to-end connectivity.
- Custom routes are displayed in Managed Desktops 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 more 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 Managed Desktops 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 Managed Desktops 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 Managed Desktops 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 Managed Desktops 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.

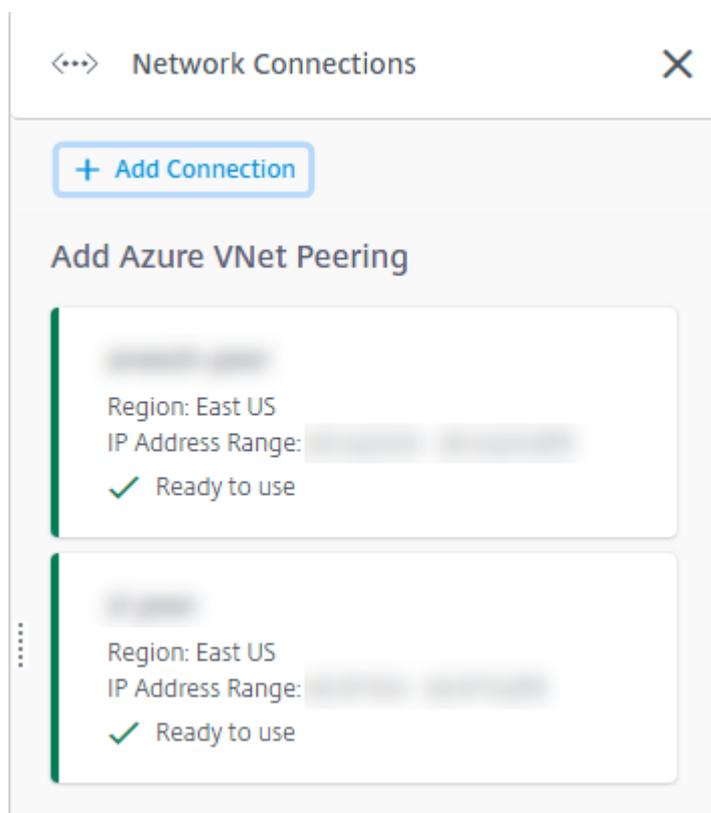
If addresses overlap, the VNet peering connection might not be created successfully. It also does not work correctly for site administration tasks.

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** dashboard, 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.

Add a network connection

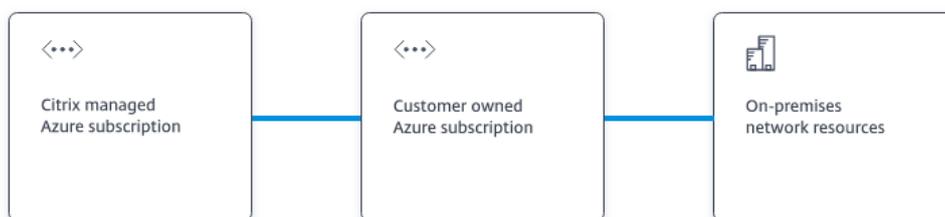
Choose how you want to connect to your local network:

Add Azure VNet Peering

Easy setup for Azure customers – Seamlessly connect your Azure virtual network.

4. Click **Authenticate Azure Account**.

Add Azure VNet Peering

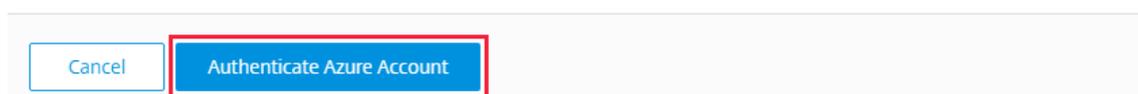


What's ahead

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

You will need the following:

1. An Azure subscription, resource group, and virtual network (VNet).
2. Credentials for an Azure Resource Manager subscription owner.
3. An available IP address and network prefix (in CIDR format) that is unique among the network resources and the Azure VNETs being connected.
4. For domain-joined scenarios, we recommend that you have some form of Active Directory services running in the peered VNet.



5. The service 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.

Add Azure VNet Peering

Azure VNet peering name

VNet details to peer

Select Azure Subscription

Select Resource Group

Select VNet to Peer

✓ This VNet is in the West US region, which is supported

Is this VNet using an Azure Virtual Network Gateway?

No Yes

IP address and network prefix to be used by VNet peering ?

⚠ The IP addresses cannot conflict with any existing IP addresses in your network.

/

?

✓ 10.2.0.0 - 10.2.0.255 (251 addresses available for machines)

Do you want to add routes? ?

No Yes

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. 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 Managed Desktops 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.

10. 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.

Do you want to add routes? 

No Yes

 Make sure your company's route tables are updated with the Citrix Managed Desktops VNet information to ensure end-to-end connectivity: 10.2.0.0/24 (provided above). Added routes override Azure default routing. Routes apply to all connections from machines using this VNet peering.

Route name

Destination IP address and network prefix 

 / 
 10.2.0.0 - 10.2.0.255

Next hop type 

Next hop address 

[+ Add route](#)

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.

11. Click **Add VNet Peering**.

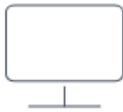
After the connection is created, it is listed under **Network Connections > Azure VNet Peers** on the right side of the **Manage** dashboard. When you create a catalog, this connection is included in the available network connections list.

View Azure VNet peering connection details

[Blurred text]

Details Routes

Not in use



Catalogs

0

Machines

0

Images

0

Bastions

0

Region

VNet 1 [Blurred]
East US

VNet 2 - CITRIX MANAGED
East US

Allocated Network Space

IP ADDRESS RANGE
[Blurred]

IP ADDRESS AVAILABLE FOR MACHINES
[Blurred]

DNS SERVERS
[Blurred]

Peered Virtual Network Details

VIRTUAL NETWORK
[Blurred]

SUBSCRIPTION ID
[Blurred]

RESOURCE GROUP
[Blurred]

AZURE VIRTUAL NETWORK GATEWAY
Disabled

Delete Connection

1. From the **Manage** dashboard, 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:

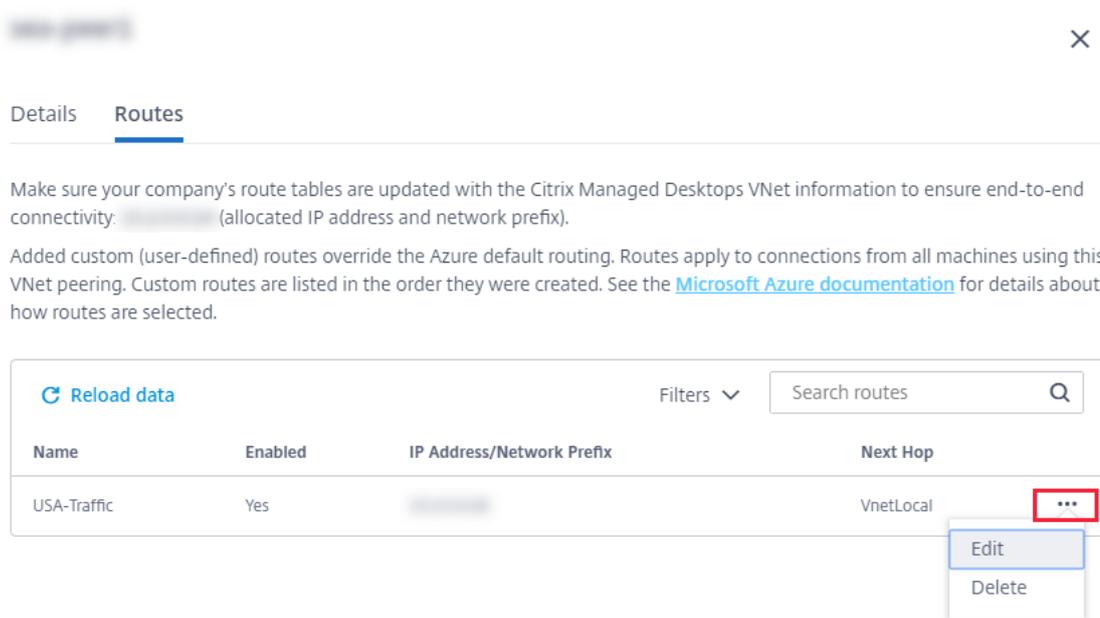
Modifying, disabling, or deleting custom routes changes the traffic flow of the connection and might disrupt any user sessions that might be active.

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](#).

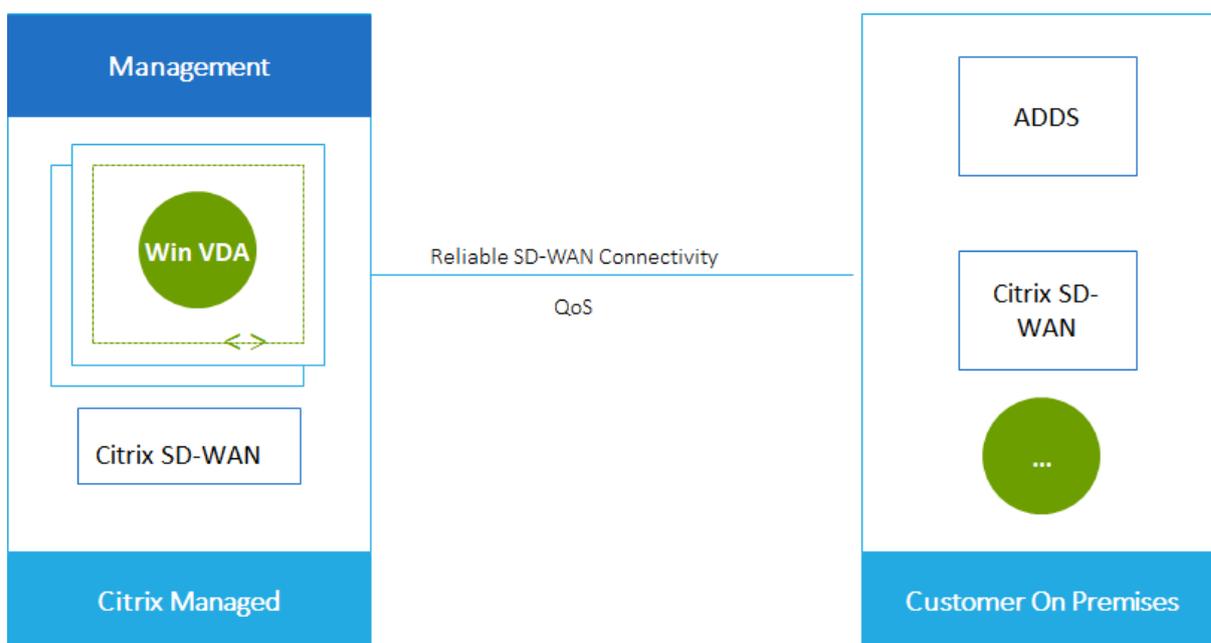
1. From the **Manage** dashboard, expand **Network Connections** on the right.
2. Select the connection you want to delete.
3. From the connection details, click **Delete Connection**.

About SD-WAN connections

Citrix SD-WAN optimizes all the network connections needed by Citrix Managed Desktops. Working in concert with the HDX technologies, Citrix SD-WAN provides quality-of-service and connection reliability for ICA and out-of-band Citrix Managed Desktops 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 Managed Desktops 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 Managed Desktops 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 Managed Desktops 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 Managed Desktops 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 CMD integration](#).

1. From the **Manage** dashboard, 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** dashboard. When you're done reading, click **Got it**.
 8. On the **Manage** 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** dashboard, 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** dashboard, 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.

Master images

April 23, 2020

When you create a catalog, a master image is used (with other settings) as a template for creating the machines.

Citrix-managed master images

Citrix Managed Desktops provides several Citrix-managed master 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

The Citrix-managed master images already have a 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 the service. Images provided by Citrix are notated as **CITRIX**.

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

Ways to use master images

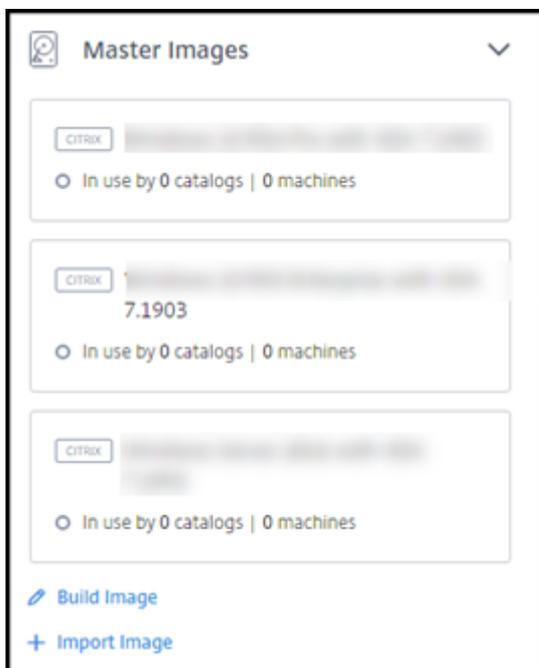
You can:

- **Use a Citrix-managed image when creating a catalog.** This choice is recommended only for proof of concept deployments.
- **Use a Citrix-managed 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 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 use that customized image when creating a catalog.

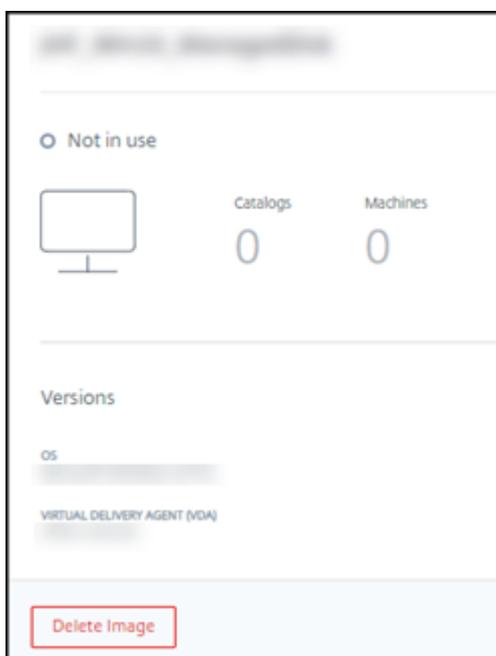
When you create a catalog, Citrix Managed Desktops verifies that the master image uses a valid operating system, and has a Citrix VDA and troubleshooting tools installed (along with other checks).

Display master image information

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



2. Click an image to display its details.



Prepare a new master image

Preparing a new master 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 master image and the catalog. For details, see [Network connections](#).

To create a master image:

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

Select a master image
Citrix Win 10 Pro 1809 + VDA 1906.2

Name The New Master Image

Choose subscription
Citrix Citrix Managed

Select a network connection ⓘ
No connectivity to corporate network

Select a region
East US

Set log-on credentials for the image machine ⓘ

Username *

Password *

Confirm password *

Select machine performance ⓘ
D2s v3 2 vCPU 8 GB RAM

3. Enter values in the following fields:

- **Master image:** Select an existing master image. This is the base image that is used to create the new master image.
- **Name:** Enter a name for the new master image.
- **Subscription:** Select either the Citrix-managed subscription or one of your customer-managed Azure subscriptions. For details, see [Azure subscriptions](#).

- **Network connection:**
 - If using the Citrix-managed subscription, select **No connectivity** or a previously created connection.
 - If using a customer-managed subscription, select your resource group, virtual network, and subnet. Then add domain details: FQDN, OU, service account name, and credentials.
- **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 master image, so that you can install apps and other software.
- **Machine performance:** Select a machine performance that meets your apps' requirements.
- **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**.

A master image can take up to 30 minutes to build. On the **Manage** 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 master image and customize it.

Connect to a new master image and customize it

After a new master image is created, its name is added to the **Master 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** 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 master 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 master image is included in the list of images you can select.

On the **Manage** dashboard, the **Master Images** display on the right indicates how many catalogs and machines use each image.

Import a master image from Azure

When you import a master 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.

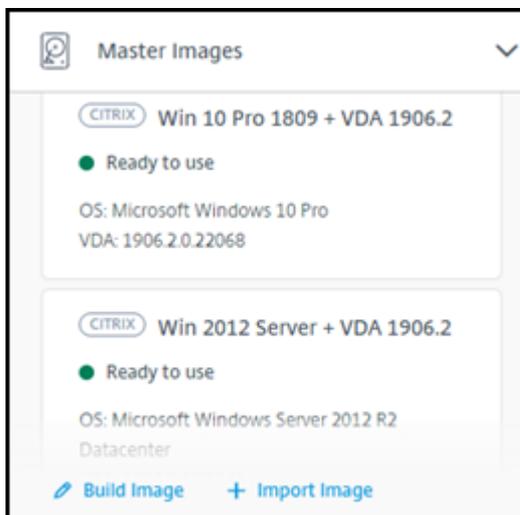
Imported image requirements

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 Managed Desktops.

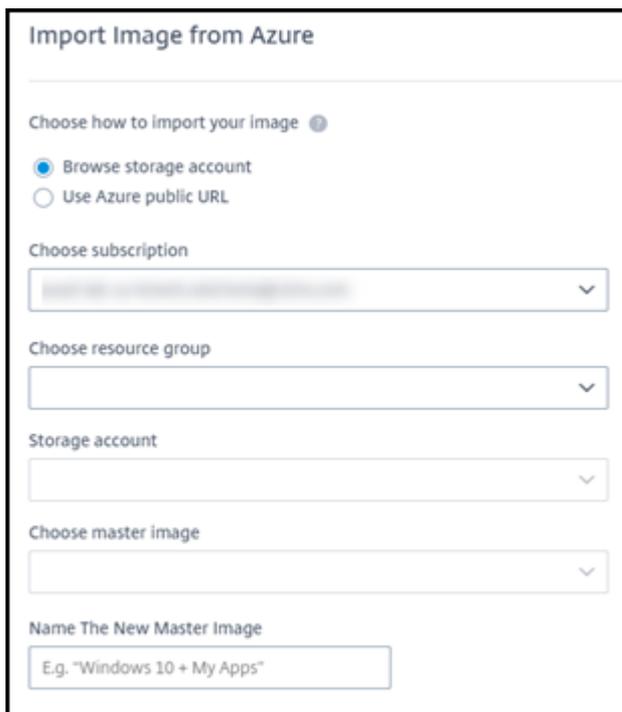
- **Supported OS:** The image must be a [supported OS](#). To check a Windows OS version, run `Get-WmiObject Win32_OperatingSystem`.
- **No configured Delivery Controllers:** Ensure that no Citrix Delivery Controllers are configured in the image. Ensure that the following registry keys are cleared.
 - `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-ItemProperty HKLM:\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\Citrix Virtual Desktop Agent`. For installation guidance, see [Install a Windows VDA on a master image](#).
 - Red Hat Enterprise Linux and Ubuntu (currently in preview): 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** dashboard, expand **Master Images** on the right.



2. Click **Import Image**.



3. Choose how the image will be imported.
 - 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 > master image.
 - b) Name the master 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 master image can be imported only if you select a customer-managed subscription.)
 - c) Name the master image.
- 6. When you're done, click **Import Image**.

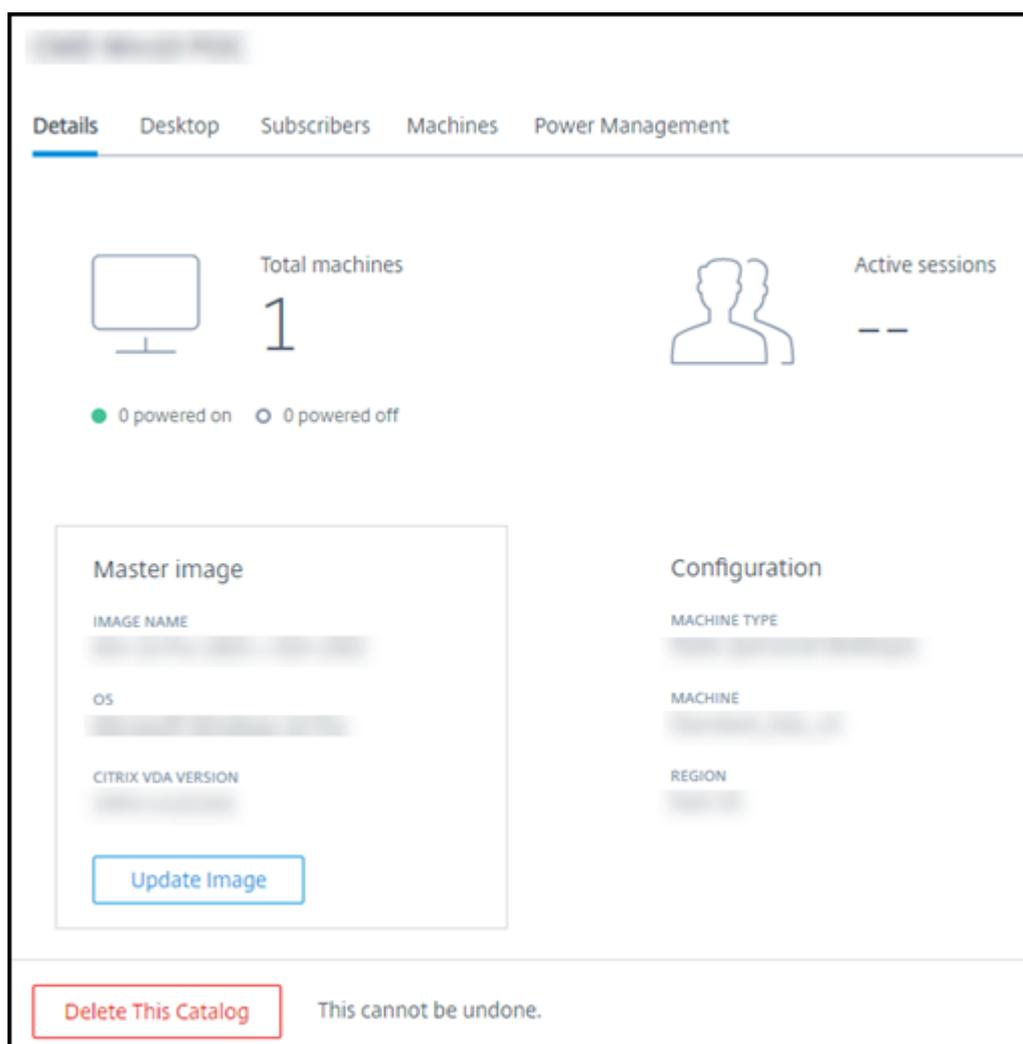
Update a catalog with a new master image

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 master 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 master image they were created from. However, if you add more machines to that catalog, they are based on the latest master image.

To update a catalog with a new master image:

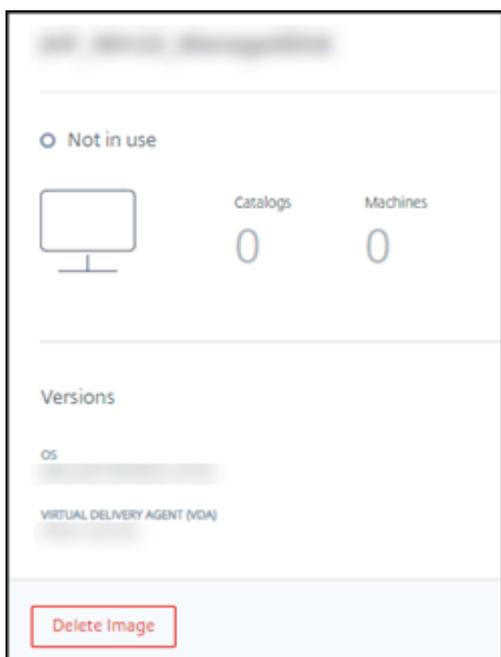
1. From the **Manage dashboard**, click anywhere in the catalog's entry.
2. On the **Details** tab, click **Update Image**.



3. Select a master image.
4. For random or multi-session catalogs: Select a logoff interval. After the service 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 a master image

1. From the **Manage** dashboard, expand **Master Images** on the right.
2. Click the image you want to delete.



3. Click **Delete Image**.

Install a Windows VDA on a master image

Use the following procedure when preparing a Windows image that you plan to import into Citrix Managed Desktops. For Linux VDA installation guidance, see the [Linux VDA product documentation](#).

1. In your environment, connect to the master 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 the Citrix Virtual Apps and Desktops service [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 **Create a master 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

April 23, 2020

User authentication methods

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

Citrix Managed Desktops 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.

Managed Azure AD is used for test or pilot deployments.

- **Your Active Directory:** If you use your own Azure subscription for catalogs and images, you can use any available authentication method in Citrix Cloud.

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:

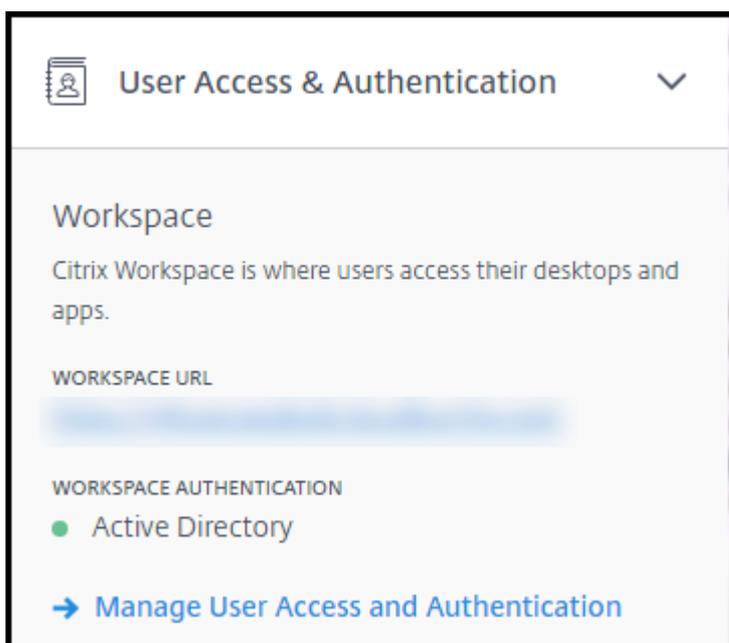
- Connect to the user authentication method you want to use. (In Citrix Cloud, you "connect" or "disconnect" from an authentication method.)
- In Citrix Cloud, set Workspace authentication to use the connected method.

Note:

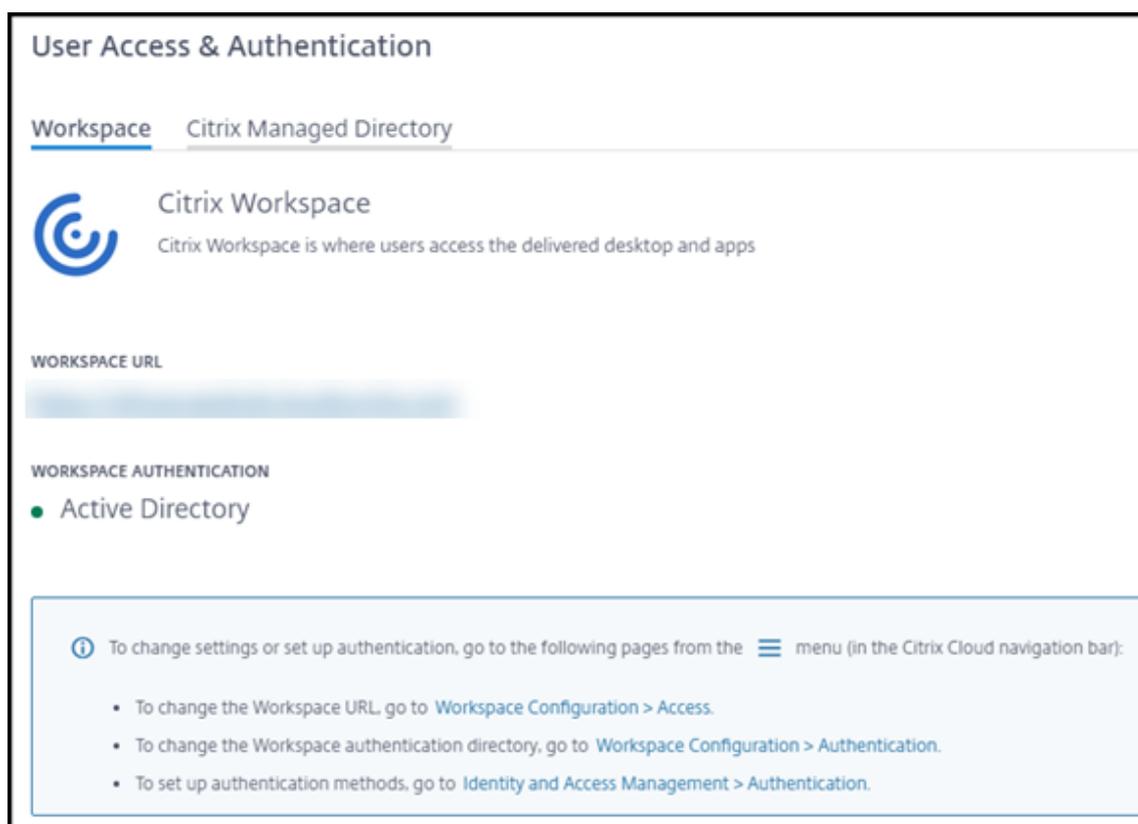
The Managed Azure AD authentication method is configured by default. That is, it is automatically connected in Citrix Cloud, and Workspace authentication is automatically set to use Managed Azure AD for this service. If you want to use this method (and have not previously configured a different method), continue with Add and delete users in Managed Azure AD.

To change the authentication method:

1. From the **Manage** dashboard, 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.

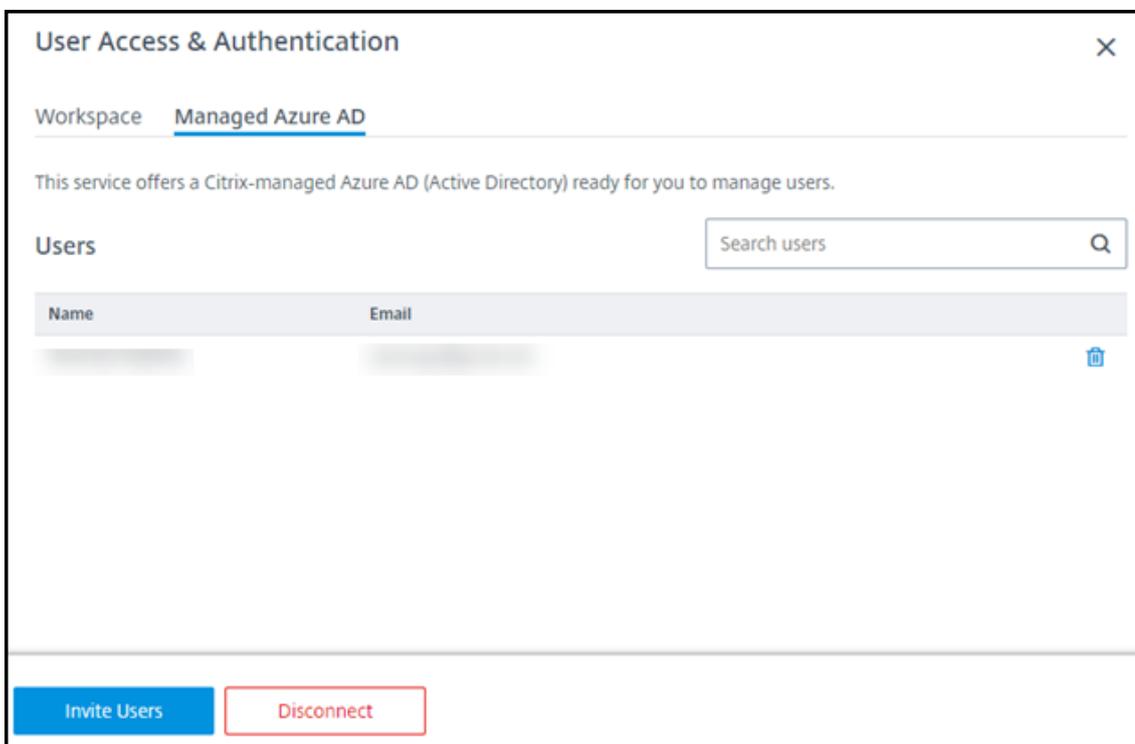
Add and delete users in Managed Azure AD

This task applies 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.

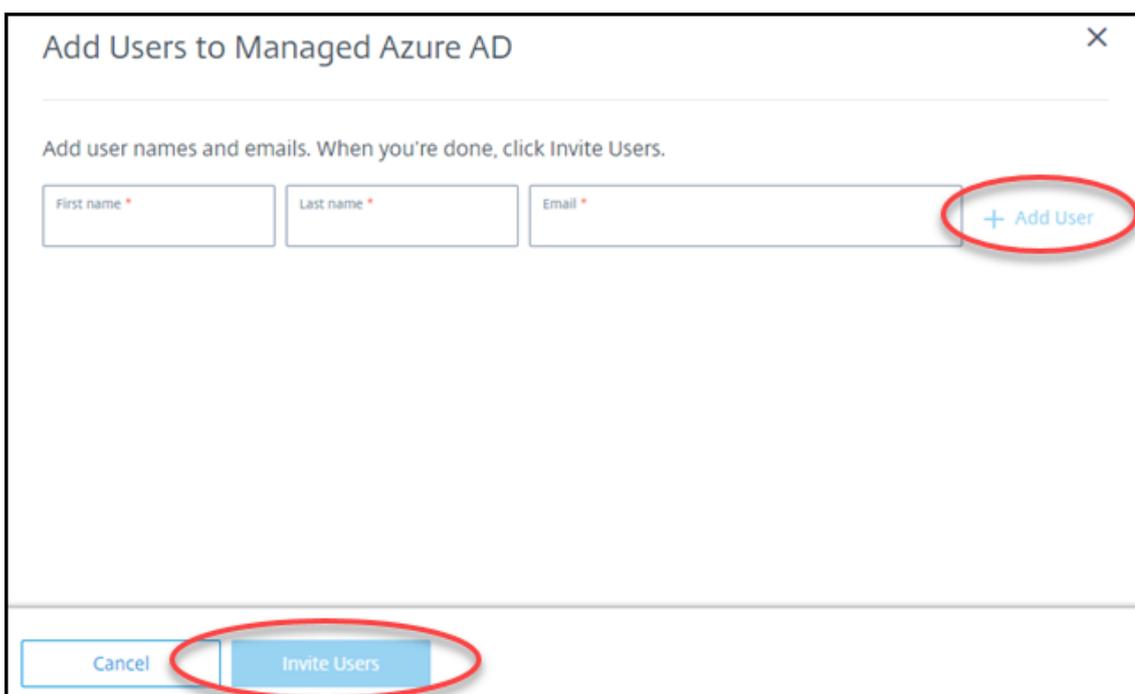
- If the user already has a Microsoft account with the email address you provided, that account is used.
- If the user does not have a Microsoft account with the email address, Microsoft creates an account.

To add and invite users to Managed Azure AD:

1. From the **Manage** dashboard, 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.

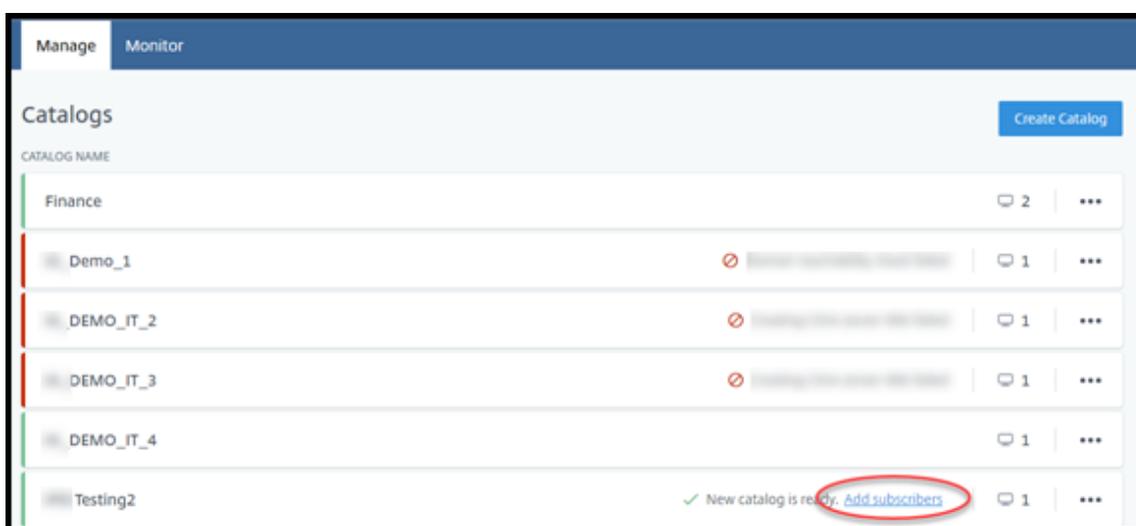
To delete a user from Managed Azure AD, click the trash icon next to the name of the user you want to delete from the directory. Confirm the deletion.

What to do next: Add users to the catalog

Add or remove users in a catalog

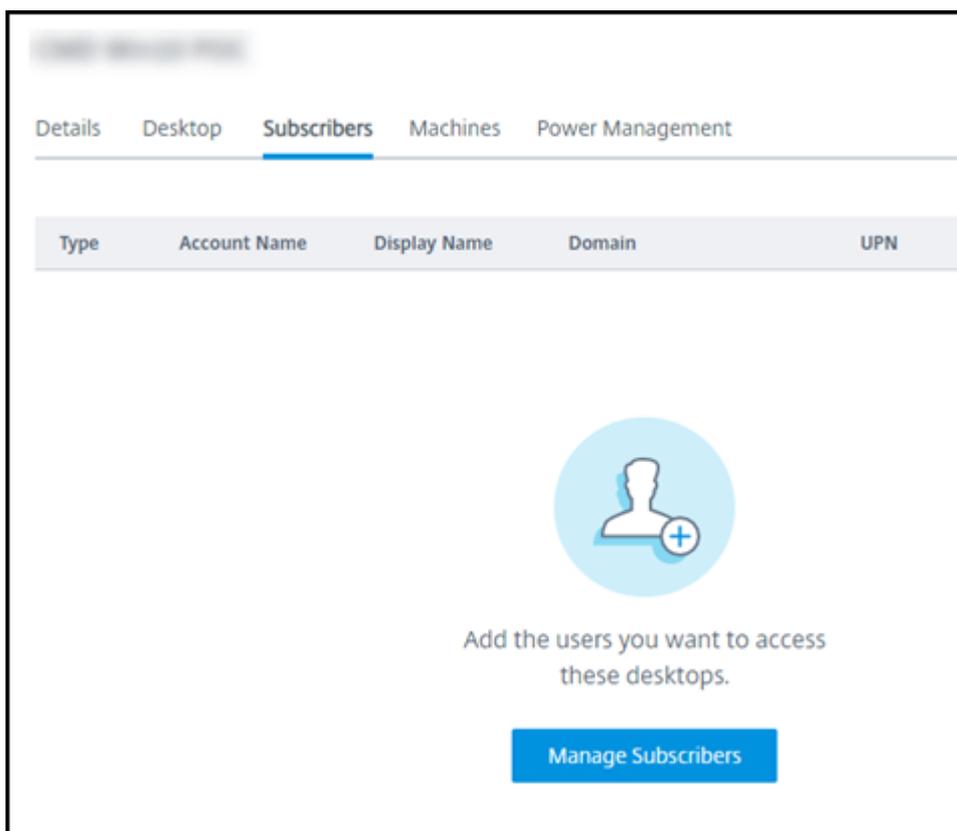
This procedure applies regardless of which authentication method you use.

1. From the **Manage** dashboard, if you haven't added any users to a catalog, click **Add subscribers**.

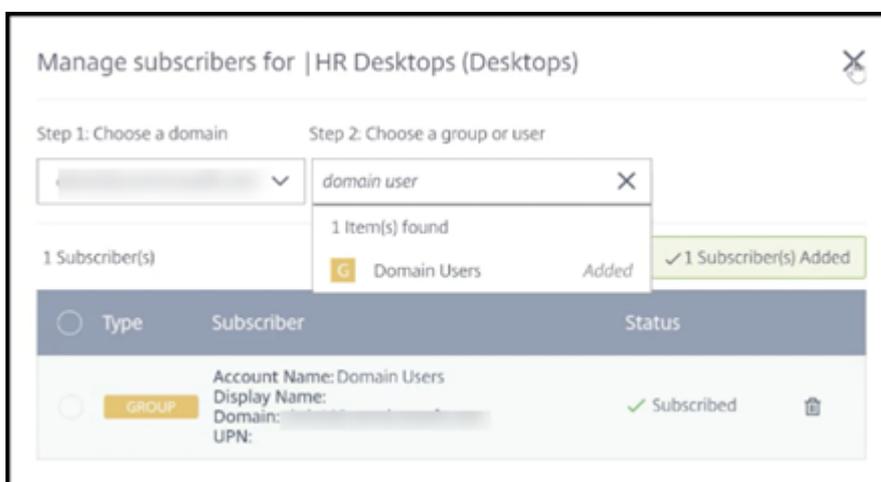


To add users to a catalog that already has users, click anywhere in the catalog's entry.

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:

- When you finish preparing a static or random catalog, send the Citrix Workspace URL to your users. On the **Manage** dashboard, the URL is on the right in **User Access & Authentication**.
- For a multi-session catalog, [add applications](#) (if you haven't already) and then [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

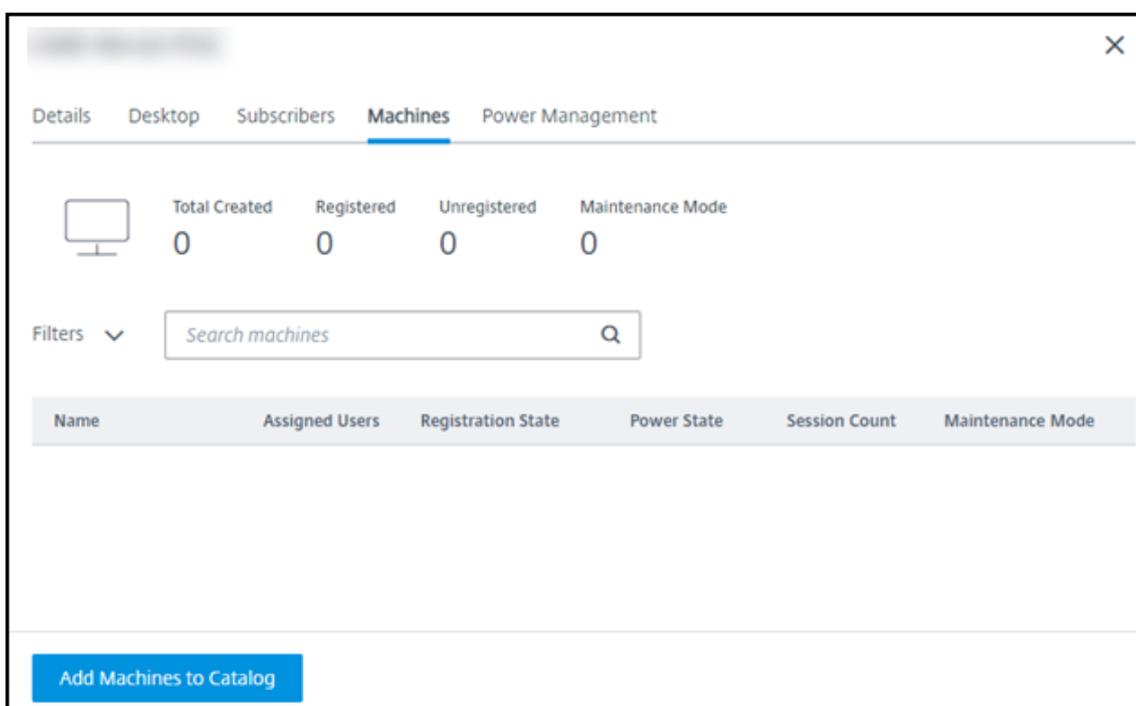
April 24, 2020

This article describes the tasks that manage catalogs and the machines they contain.

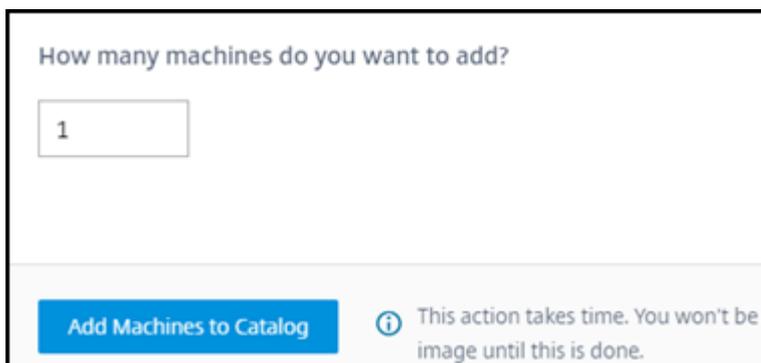
Add machines to a catalog

Adding machines to a catalog can take a while. During that interval, you cannot make any other changes to that catalog.

1. From the **Manage** 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.



The screenshot shows a dialog box with the title "How many machines do you want to add?". Below the title is a text input field containing the number "1". At the bottom of the dialog, there is a blue button labeled "Add Machines to Catalog" and a warning message: "This action takes time. You won't be able to use the image until this is done." The warning message is preceded by an information icon (i).

4. (Valid only if the catalog is domain-joined.) Type the username 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.

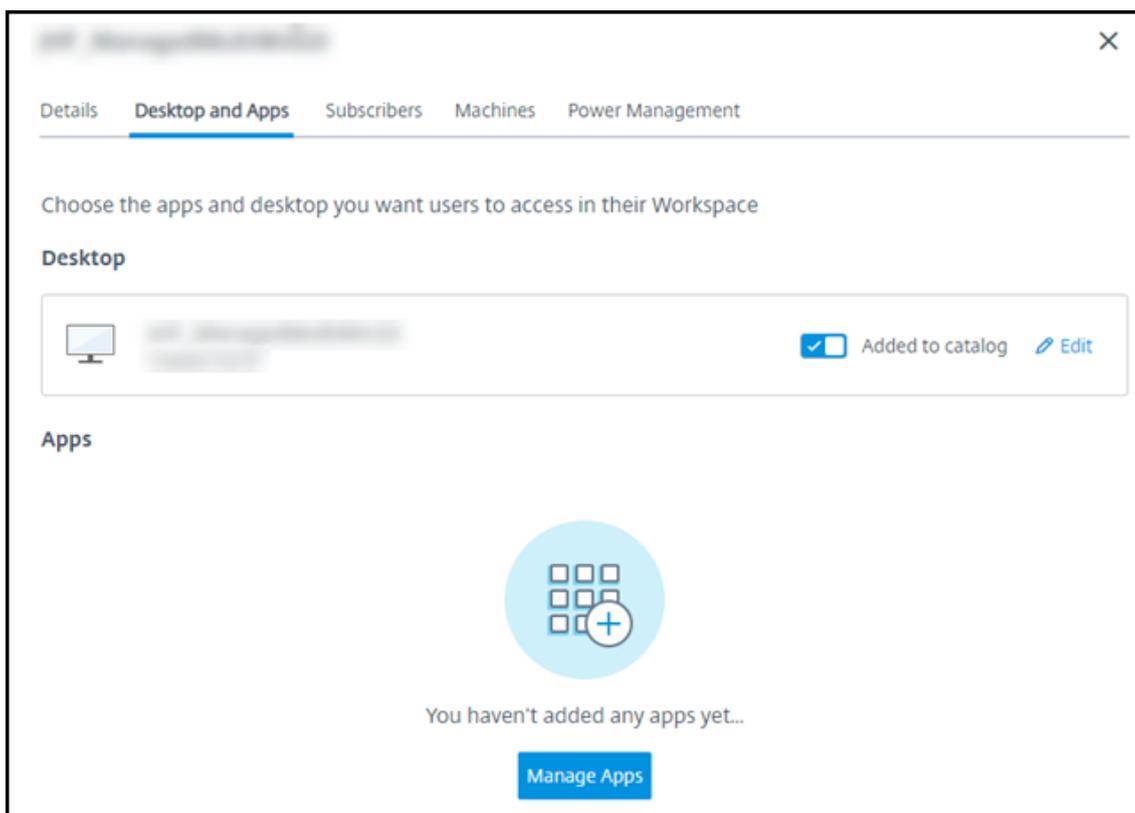
Delete machines from a catalog

You can delete a machine only when it has no sessions. When a machine is deleted, all data on the machine is removed.

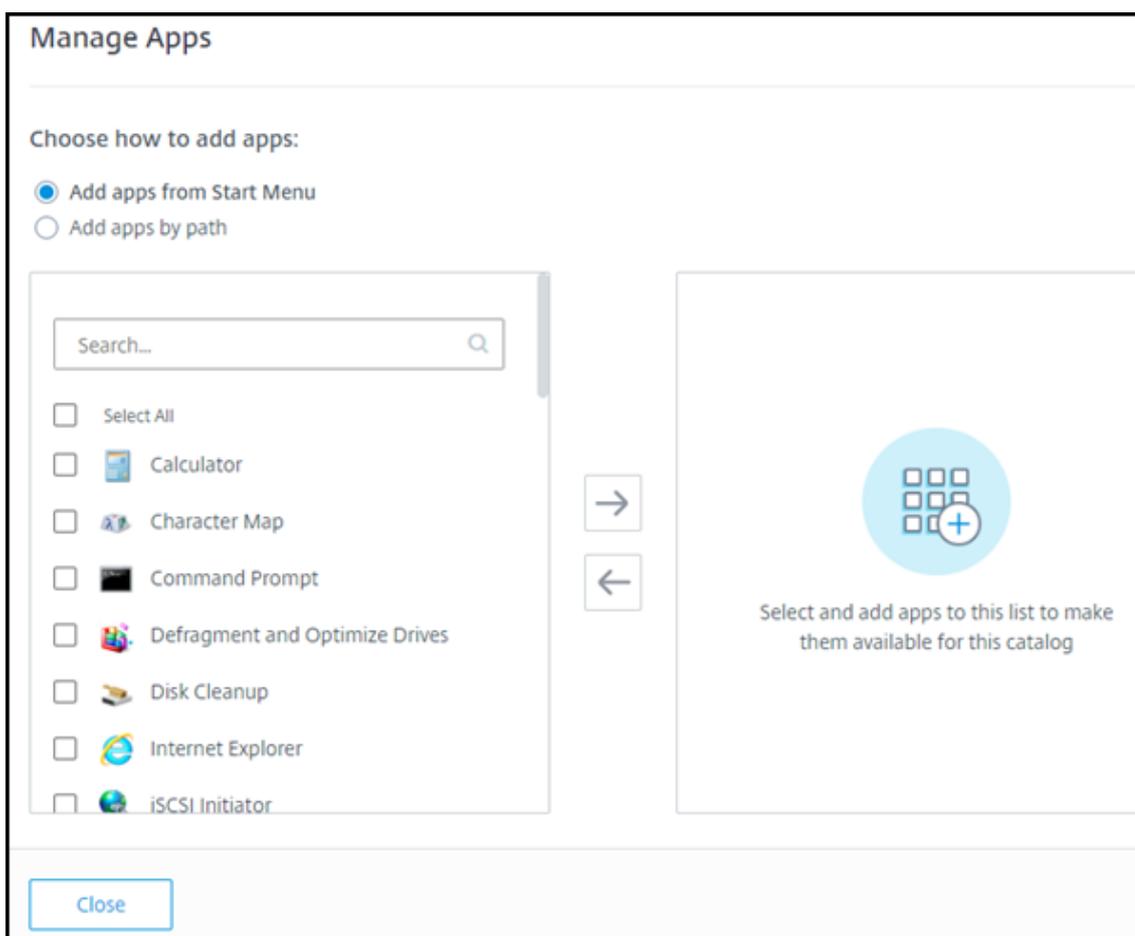
1. From the **Manage** dashboard, click anywhere in the catalog's entry.
2. On the **Machines** tab, select **Delete** in the ellipsis menu for the machine you want to delete. (Only machines with a zero session count can be selected for deletion.)
3. Confirm the deletion by selecting the check boxes and then click **Yes, Delete It**.

Add apps to a catalog

1. From the **Manage** 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:

Manage Apps

Choose how to add apps:

Add apps from Start Menu

Add apps by path

Enter the App Details Displayed to Users

App Name *

 [Change Icon](#) ⓘ

Description

Enter the App Parameters

Path *

Command Line Parameters:

Working Directory:

Close

Select and add apps to this list to make them available for this catalog

- 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.

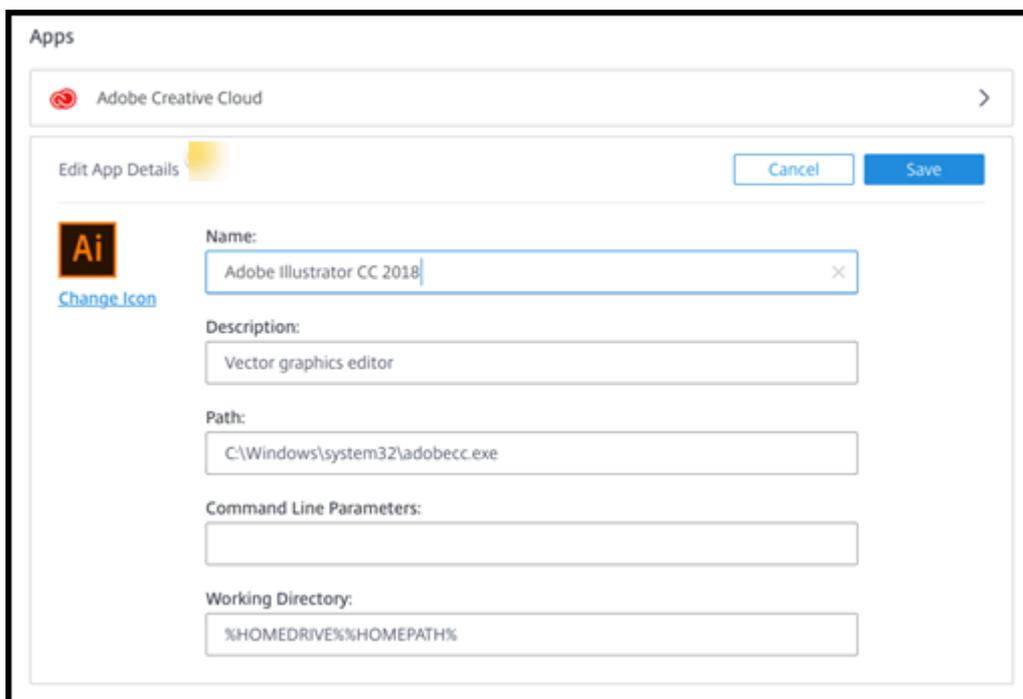
6. When you're finished, click **Close**.

What to do next: [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** 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.



The screenshot shows a dialog box titled "Apps" with a sub-header "Adobe Creative Cloud". Below this is a section titled "Edit App Details" with "Cancel" and "Save" buttons. The app icon is "Ai" with a "Change Icon" link. The fields are:

- Name: Adobe Illustrator CC 2018
- Description: Vector graphics editor
- Path: C:\Windows\system32\adobecc.exe
- Command Line Parameters: (empty)
- Working Directory: %HOMEDRIVE%\%HOMEPATH%

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** 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** dashboard, click anywhere in the catalog’s entry.
2. On the **Details** tab, click **Delete This Catalog** on the lower portion of the window.
3. Confirm the deletion by selecting the acknowledgment check boxes and then clicking the confirmation button.

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.

The screenshot shows the 'Power Management' configuration page in Citrix Managed Desktops. At the top, there are navigation tabs: 'Details', 'Desktop and Apps', 'Subscribers', 'Machines', and 'Power Management'. Below the tabs, the 'Presets' section shows 'Cost Saver' selected. The 'General' section includes three dropdown menus: 'Disconnect desktop sessions when idle' (After 15 Minutes), 'Log Off Disconnected Sessions' (After 15 Minutes), and 'Power Off Delay' (After 30 Minutes). The 'Work hours' section features a 'Time Zone' dropdown set to '(UTC-05:00) Eastern Time (US & Canada)', a 'Power on machines' section with buttons for SUN, MON, TUE, WED, THU, FRI, and SAT, and 'Start' and 'End' time dropdowns. Below this are 'Capacity buffer' (10%) and 'Minimum running machines' (1) input fields. The 'After-hours' section has similar 'Capacity buffer' (10%) and 'Minimum running machines' (1) settings. A 'Save Changes' button is located at the bottom left.

A power management schedule contains the following information.

Preset schedules

Citrix Managed Desktops 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 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%, the service 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. This 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. This means that 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** 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 click **Save current settings as 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.

Related information

- [Update a catalog with a new master image](#)
- [Add and remove users in a catalog](#)
- [Domain-joined and non-domain-joined](#)

Monitor

September 30, 2019

From the **Monitor** dashboard, you can view desktop usage, sessions, and machines in your Citrix Managed Desktops 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 > Managed Desktops**.
2. From the **Manage** dashboard, click the **Monitor** tab.

Several displays refer to *Delivery Groups* and catalogs. In Citrix Managed Desktops, these terms are equivalent.

Monitor desktop usage

The **Managed Desktop Usage** page appears by default when you click the **Monitor** tab. Displays on this page refresh every five minutes.

To return to the **Managed Desktop Usage** page from any other Monitor dashboard display, click **Usage**.

- **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, month, or three months.

Counts at the top of the display indicate the total number of machines, plus the number 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 Frequent 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 desktop launches during the last month, click **Desktop Launch Activity** on the **Managed Desktop Usage** page. 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

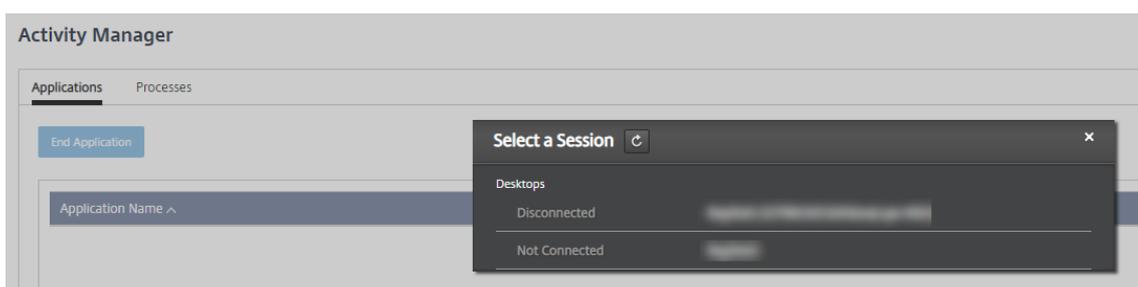
When you're monitoring session and machine information, all machines or sessions are displayed by default. You can:

- Filter the display by session or machine type.
- 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

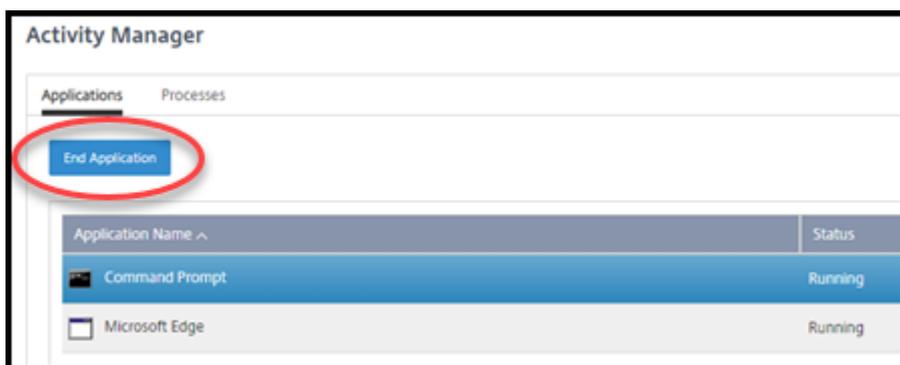
You can display and manage applications and processes for a user that has a running session or an assigned desktop.

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



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**.



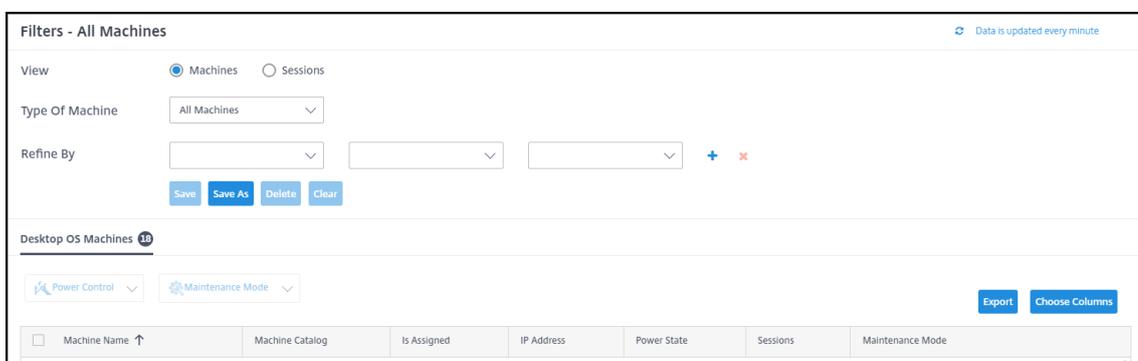
4. To end a process, on the **Processes** tab in Activity Manager, click in the process's row to select that process, and then click **End Process**.
5. To display session details, click **Details** in the upper right. To return to the applications and processes display, click Activity Manager in the upper right.
6. To control the session, click **Session Control > Log Off** or **Session Control > Disconnect**.

Monitor and control sessions

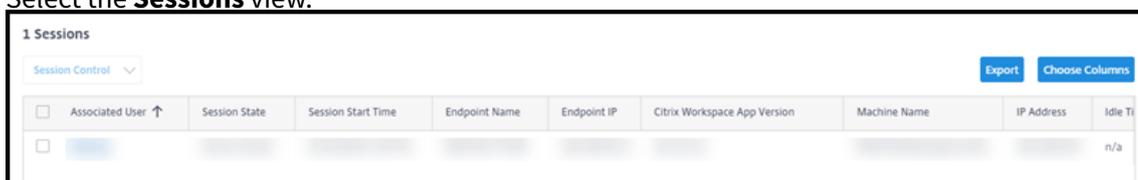
Session displays are updated every minute.

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

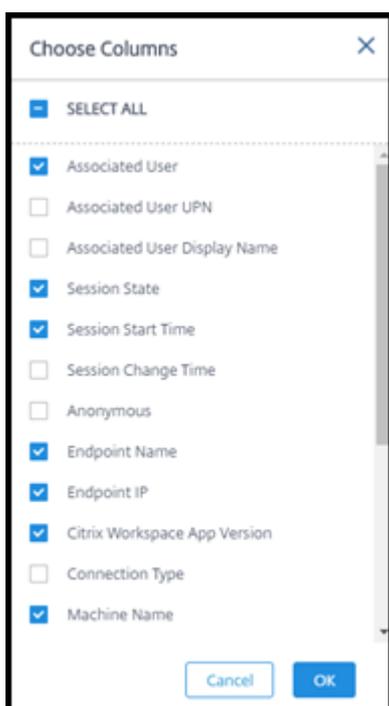
1. From the **Monitor** dashboard, click **Filters**.



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.

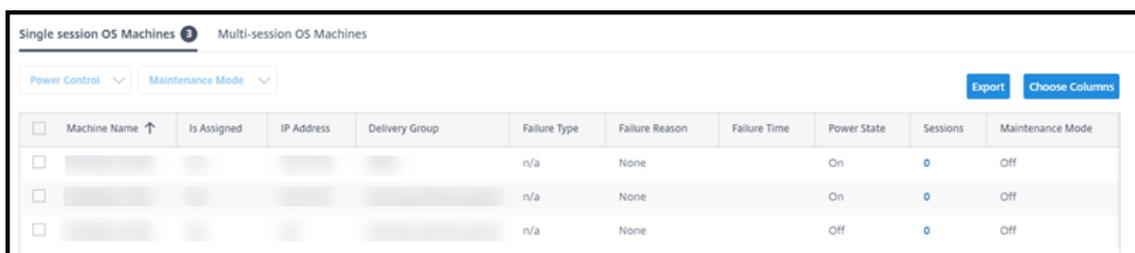
Session information report

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

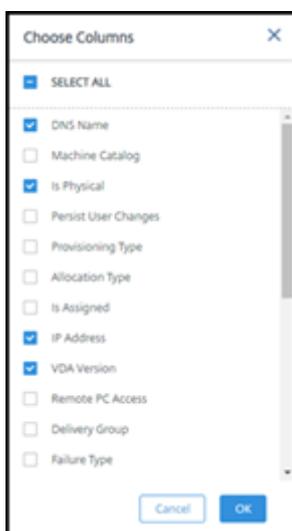
Machine displays are updated every minute.

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**.

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.

Citrix Managed Desktops service for Citrix Service Providers

April 1, 2020

This article describes how Citrix Service Providers (CSP) can set up the Citrix Managed Desktops service for tenant customers 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 Managed Desktops.

Limitations

- Tenant name changes take up to 24 hours to apply across all interfaces.
- When creating a tenant, the email address must be unique.
- Management filtering by tenant is not available. To see the resources attached to a tenant, select Show items for in the management pane.

Known issues

- After a tenant is assigned to a resource, you cannot remove or unassign them.
- The management console does not enforce tenant user separation. You are responsible for adding users to the appropriate catalogs and resources.
- After adding Citrix Managed Desktops to a customer:
 - You cannot remove it from a customer.
 - You cannot remove the link between the customer and the CSP.

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 Managed Desktops **Manage** and **Monitor** dashboards.

Add Citrix Managed Desktops 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 Managed Desktops**.
4. Click **Continue**.

After you complete this procedure, the customer is onboarded to your Citrix Managed Desktops subscription.

When the onboarding completes, a new tenant is created automatically in the Citrix Managed Desktops. The tenant is visible in the management console. This tenant is unique to that customer.

Filter resources by customer (multitenant deployments)

You can filter resources by customer on the Citrix Managed Desktops **Manage** dashboard. (By default, all resources are displayed.) When working with resources such as catalogs, master images, and Azure subscriptions, you can select specific customer displays to help organize your tenants' resources.

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, a master 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 Managed Desktops, as needed.
7. When you're done, click **Send Invite**.

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

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 the service, 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 tenant 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 Managed Desktops:** On the **Manage** 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 Managed Desktops **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.

Troubleshoot

April 23, 2020

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, too. 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 in the Citrix-managed Azure subscription. For details, see:

- Resource location actions available from the Manage dashboard
- [Resource location settings when creating a catalog](#)

Citrix Managed Desktops also 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 dedicated Citrix-managed Azure subscription through a bastion machine or direct RDP. After gaining access to the subscription, Citrix supportability tools are used to locate and resolve issues. For details, see:

- VDA troubleshooting using a bastion or direct RDP
- Bastion access
- Direct RDP access

Resource location actions from the Manage dashboard

1. From the **Manage** dashboard, expand **Subscriptions** on the right.
2. Click the Citrix-managed subscription.

The **Resource Locations** tab on the subscription card lists each resource location, plus the status of each Cloud Connector in the resource location.

Each resource location's entry contains an ellipsis menu. From this menu, you can select the following actions.

- **Run Health Check:** Selecting this action in the menu 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. After selecting this action in the menu, 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.

After selecting this action in the menu, provide the following information.

- How many Cloud Connectors to add.
- The OU for the Cloud Connectors. By default, the resource locations' OU is used.
- Whether your network requires a proxy server for internet connectivity. If it does, enter the proxy server's FQDN or IP address, including the port number.
- The domain service account name and password. These credentials are used to domain-join the Cloud Connector machines.

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.

After selecting this action in the menu, select the check box for the Cloud Connector you want to delete. Then click **Delete**.

(You can also delete an available Cloud Connector. However, if deleting the selected available Cloud Connector will result in fewer than two available Cloud Connectors in the resource location, you cannot 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.

After selecting this action in the menu, choose the time to begin updates, or indicate that you want updates to start when an update is available. Click **Save**.

- **Rename:** After selecting this action in the menu, enter the new name for the resource location. Click **Save**.
- **Configure Connectivity:** After selecting this action in the menu, indicate whether users can access desktops and apps through the Citrix Gateway service, or only from within your corporate network.

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 Virtual Apps and Desktops 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 Citrix-managed dedicated customer 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 master image machines.

- Direct RDP access to the machines in the Citrix-managed dedicated customer 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** dashboard, 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** dashboard, 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 with Citrix Managed Desktops, open a ticket by following the instructions in [How to Get Help and Support](#).

Limits

June 17, 2020

This article lists the limits for various resources in a Citrix Managed Desktops service deployment.

Site-level configuration limits

The following table lists the limits for site-level resources.

Resource	Limit
Active Directory domains	25
Catalogs	100
Resource locations	25
VDAs per subscription	1,200

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	5,000
Multi-session VDAs	500

Provisioning limits

The limits in the following table are 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	1,000
VDAs per Microsoft Azure subscription	1,000

Site-level usage limits

Resource	Limit
Concurrent Monitor full administrators	5
Concurrent end users	25,000
Resources published to a single user	250
Session launches per minute	2,000

Trial limits

The following table lists the limits during a Citrix Managed Desktops service trial.

Resource	Limit
Maximum number of catalogs	3
Maximum number of users	25
Maximum number of VDAs per catalog	3

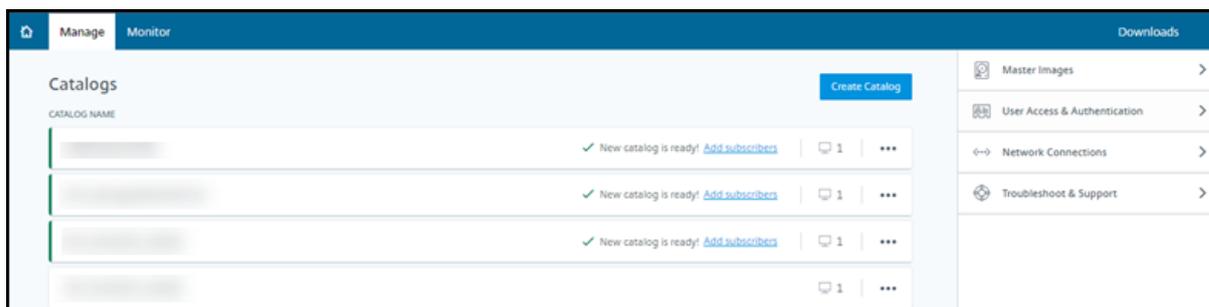
Reference

May 5, 2020

Dashboards

Most of the administrator activities for this service are managed through the **Manage** and **Monitor** dashboards. After you create your first catalog, the **Manage** dashboard launches automatically after

you sign in to Citrix Cloud and select the **Managed Desktops** service.



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 > Managed Desktops**. (Alternatively, you can click **Manage** on the **Managed Desktops** 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** dashboard.
4. If a catalog has already been created, you're taken automatically to the **Manage** 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** dashboard in Citrix Managed Desktops, click anywhere in the catalog's entry. The following tabs contain information about the catalog:

Details

The **Details** tab lists the information specified when the catalog was created (or its most recent edit). It also contains information about the master image that was used to create the catalog.

From this tab, you can:

- [Change the master image](#) that is used in the catalog.
- [Delete the catalog](#).

Desktop

The **Desktop** tab is 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

The **Subscribers** tab 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

The **Machines** tab 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, assigned user, registration state (registered/unregistered), power state (on/off), session count (0/1), maintenance mode (on/off).

You can filter searches by session count, power state, registration state, and maintenance mode state.

From this tab, you can add machines to the catalog, remove machines from a catalog, and turn maintenance mode on or off for one or more machines.

Maintenance mode

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

You can turn maintenance mode on or off for machines from a catalog's **Details** tab on the **Manage** dashboard.

You can also monitor machines and turn maintenance mode on or off from the **Monitor** tab. For details, see [Monitor and power control machines](#).

Power Management

The **Power Management** page 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 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

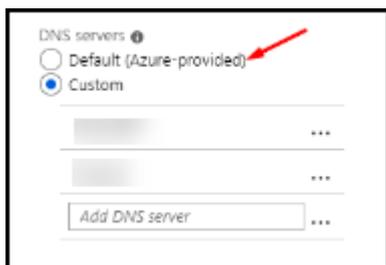
This section applies to all deployments that contain domain-joined machines. (See [Domain-joined and non-domain-joined](#).) You can ignore this section if you use only non-domain-joined machines.

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 Managed Desktops 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 Managed Desktops 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 Managed Desktops 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 Managed Desktops.
- When using a Citrix-managed Azure subscription, Citrix Managed Desktops does not synchronize DNS address changes that you make in Azure. However, you can change DNS settings for the connection in Citrix Managed Desktops.

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 Managed Desktops

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** 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 master image.
2. On the master image machine, 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. Using the **Run** command, launch `gpedit.msc` to open the Group Policy Editor.
4. In `User Configuration Citrix Policies > Unfiltered`, click **Edit Policy**.
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 master image.
7. Either [update the existing catalog](#) or [create a new catalog](#) using the new master image.

Set group policies for domain-joined machines

1. Ensure that the Group Policy Management feature is installed on the machine:
 - 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, 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 Managed Desktops, see the [Policy settings reference](#) articles to learn about what's available.

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 log on and log off 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

Citrix Managed Desktops 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 VDA 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 Citrix Managed Desktops apply the license server settings. You can configure the license server and per user mode in the RDS console on the master 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.

Monitor Citrix license usage

To view your Citrix license usage information, follow the guidance in [Monitor licenses and active usage for Citrix Managed Desktops service](#). You can view:

- Licensing summary
- Usage reports
- Usage trends and license activity
- Licensed users

Load balancing

Note:

Load balancing applies to multi-session machines, not single-session machines. The selection of load balancing method applies to all catalogs in your Citrix Managed Desktops deployment.

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 Citrix Managed Desktops 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 Managed Desktop 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** 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**.

Cancel a monthly subscription

Citrix Managed Desktops offers monthly and annual subscriptions. Annual subscriptions expire at the end of the defined contract period. Monthly subscriptions renew automatically at the beginning of each month.

To cancel a monthly subscription:

1. Sign in to [Citrix Cloud](#).
2. In the upper left menu, select **My Services > Managed Desktops**.
3. From the **Manage** 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.
6. Indicate why you're canceling the service. Optionally, provide more feedback.
7. Click **Cancel Subscription**.
8. Confirm that you understand the terms of the cancellation.

A banner on the 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 the service.

Get help

- Review the [Troubleshoot](#) article.
- If you need further assistance with Citrix Managed Desktops, open a ticket by following the guidance in [How to Get Help and Support](#).

**Locations**

Corporate Headquarters | 851 Cypress Creek Road Fort Lauderdale, FL 33309, United States

Silicon Valley | 4988 Great America Parkway Santa Clara, CA 95054, United States

© 2020 Citrix Systems, Inc. All rights reserved. Citrix, the Citrix logo, and other marks appearing herein are property of Citrix Systems, Inc. and/or one or more of its subsidiaries, and may be registered with the U.S. Patent and Trademark Office and in other countries. All other marks are the property of their respective owner(s).