Citrix DaaS Flex

Copyright © 1997–2026. Citrix Systems, Inc. All Rights Reserved.

Contents

Citrix DaaS Flex overview 2

Citrix DaaS Flex for Azure 4

What's new 9

Limits 13

Technical security overview 13

Firewall policy for Citrix DaaS Flex 20

Get started 22

Azure subscriptions 24

Network connections 26

Resource locations 62

Customer-managed encryption keys for VM disks 63

Images 66

Create catalogs and add users 78

Manage catalogs 84

Monitor 97

Delegated administration 98

Microsoft Entra ID 105

Troubleshoot 107

Citrix DaaS Flex for AWS (Tech Preview) 114

Important information and documents 115

Service Level Agreement 115

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Citrix DaaS Flex overview

July 24, 2026

Citrix DaaS Flex is the simplest, fastest way to deliver virtual apps and desktops to any device. Delivered through Citrix Cloud, this persona-based service streamlines your operations with cloud-based management, rapid provisioning, and fully managed capacity.

Citrix DaaS Flex includes:

- Cloud-based management and provisioning of VDAs hosted in Citrix-managed cloud subscriptions.
- High-definition user experience across a broad range of devices.
- Simplified image lifecycle management using Citrix-prepared and customer-provided images.
- Integrated monitoring and operational visibility.
- Compatibility with existing Citrix DaaS architectures.

Concepts and terminology

This section defines the terms that administrators frequently use on Citrix DaaS Flex.

Catalogs

A catalog is the combination of a host connection, machine catalog, and a delivery group in Citrix DaaS. Virtual Delivery Agents (VDAs) are provisioned in a Citrix DaaS Flex catalog. Applications and desktops that are delivered to end users are configured through the catalog. See Create a catalog for more information.

Images

Images are used as a template for provisioning VDAs to the Citrix DaaS Flex catalog. Citrix DaaS Flex provides two image options:

- You can import and use your own images from Azure. You must install the VDA software on the image before it can be used to create a catalog.
- Use Citrix prepared images. Currently supported images prepared by Citrix:
  - Windows 11 Pro (single-session)
  - Windows Server 2019 (multi-session)
  - Windows Server 2022 (multi-session)

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- Windows Server 2025 (multi-session)
- Linux Ubuntu 22.04 LTS (single-session)
- Linux Ubuntu 22.04 LTS (multi-session)

The Citrix prepared images have a current version of the Citrix Virtual Delivery Agent (VDA) and Citrix Optimizer. The VDA is the communication mechanism between your users' machines and the Citrix Cloud infrastructure. Citrix updates the available prepared images when a new VDA version is released.

Microsoft Licensing requirements

> **Note:**
>
> The following requirements are specific to Citrix DaaS Flex personas involving Citrix Managed Azure capacity.

- **Windows 11 single-session**: Requires a customer-provided license before use (Microsoft 365 E3/E5/E7, Microsoft 365 F3, Windows 11 Enterprise E3/E5, or Windows 11 VDA E3/E5).
- **Windows Server multi-session**: Citrix provides the required Remote Desktop Services and Server OS licensing.

Alternative deployment models

- **Bring Your Own Infrastructure (BYO)**: In scenarios where a customer uses a Bring Your Own Infrastructure model with Citrix DaaS Flex, the standard Microsoft licensing requirements that apply to traditional Citrix DaaS applies.
- **Customer-Owned Azure subscriptions**: In cases where a customer uses Citrix DaaS Flex deployed on a customer-owned Azure subscription, they can leverage all of the entitlements and benefits of the Microsoft Azure Virtual Desktop (AVD) provider.

For more information, see Images.

Azure subscriptions

The VDAs are hosted in a Citrix DaaS Flex subscription. When Citrix Platform Flex credits are purchased, a Citrix DaaS Flex subscription is assigned to your Citrix DaaS customer subscription. To maintain the privacy of your data, the Azure subscription assigned to your customer is dedicated solely to your resources.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Network connections

When creating a catalog using a Citrix DaaS Flex subscription, you indicate if and how users can access locations and resources on their corporate on-premises network from their published desktops and apps. The available options are:

- No connectivity
- Azure virtual network peering
- Azure VPN gateway
- Azure Virtual WAN spoke

For more information, see Network connections.

More information

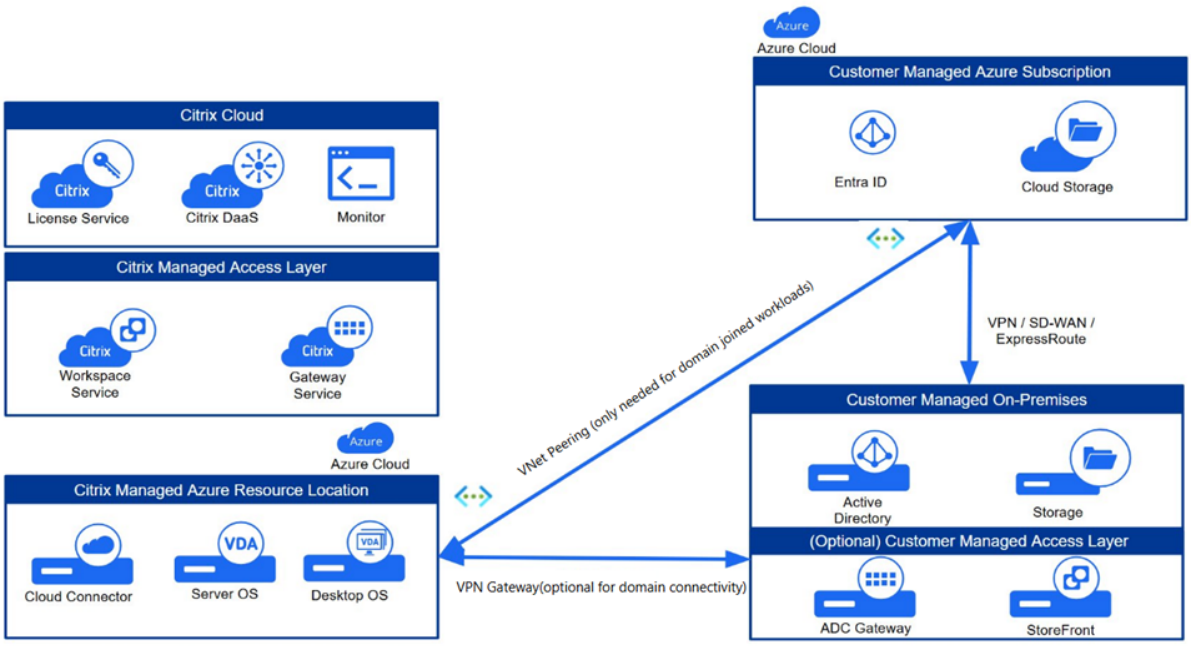
- Licensing for Citrix Platform Flex
- Platform Flex Credit consumption and reporting

Citrix DaaS Flex for Azure

September 9, 2026

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Architecture overview



Machine identity

VDAs in a Citrix DaaS Flex subscription can be:

- Non-domain joined
- Active Directory joined
- Microsoft Entra hybrid joined
- Microsoft Entra ID joined

The following table outlines the availability of the machine identity based on delivery model and network connectivity:

Single-session vs Multi-session	Persistent vs Non-persistent	Non-domain joined	Active Directory joined	Entra hybrid joined	Entra ID joined
		With network connectivity			
Multi-session	Persistent	Yes	Yes	Yes	Yes
Multi-session	Non-persistent	Yes	Yes	Yes	Yes
Single-session	Persistent	Yes	Yes	Yes	Yes

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Single-session vs Multi-session	Persistent vs Non-persistent	Non-domain joined	Active Directory joined	Entra hybrid joined	Entra ID joined
Single-session	Non-persistent	Yes	Yes	Yes	Yes
		Without network connectivity			
Multi-session	Persistent	Yes	No	No	Yes
Multi-session	Non-persistent	Yes	No	No	Yes
Single-session	Persistent	Yes	No	No	Yes
Single-session	Non-persistent	Yes	No	No	Yes

> **Note:**
>
> Intune enrollment is only supported for persistent workloads.

Non-domain-joined

Non-domain-joined VDAs are ideal for situations in which VDAs do not require direct connectivity to Active Directory or application data residing in your corporate network. While non-domain-joined VDAs can improve security by isolating VDAs from Active Directory, they lose the ability to authenticate to internal applications using Kerberos authentication. Additionally, Group Policy Objects (GPOs) cannot be configured centrally through Active Directory when using non-domain-joined machines. Administrators cannot connect directly to non-domain-joined VDAs through a bastion machine or RDP. Citrix Profile Management is not supported for non-domain-joined catalogs, so it is recommended that non-domain-joined VDAs be persistent and static

Active Directory domain-joined

Integrating VDAs with Active Directory unlocks key operational capabilities, including centralized management through GPOs and secure network authentication using Kerberos.

Active Directory domain-joined VDAs require network connectivity between the Citrix DaaS Flex subscription and the Domain Controllers.

When Citrix Workspace or StoreFront is configured to use an authentication method other than Active Directory or Entra ID, a seamless single sign-on experience requires the implementation of the Federated Authentication Service (FAS).

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Microsoft Entra hybrid joined

Joining Citrix VDAs to both Active Directory and Microsoft Entra provides users with seamless single sign-on (SSO) to all company resources, from legacy on-premise applications to modern cloud services like Microsoft 365. This hybrid strategy allows you to continue using established Group Policy management while layering on powerful cloud security like Conditional Access and MFA.

Network connectivity to Active Directory is required to hybrid-join VDAs. SCCM co-management is required if VDAs are also enrolled in Intune. See Hybrid Azure AD joined catalogs enrolled in Microsoft Intune for more information regarding hybrid joined VDAs and Intune.

Microsoft Entra ID joined

Adding VDAs to a Microsoft Entra tenant can enhance security and user experience in your environment. Joining VDAs to your Microsoft Entra tenant requires the following prerequisites:

- Entra ID Authentication
  - VDA version 2511
  - Microsoft Entra Service Account with `Device.ReadWrite.All` or equivalent role-based permissions
- Intune Device Enrollment (Optional)
  - VDA version 2603
  - Device Management Service Account with `DeviceManagementManagedDevices.ReadWrite.All` permissions

> **Note:**
>
> Adding VDAs to your Microsoft Entra tenant does not require network connectivity between your VDAs and your network.

Intune enrollment

Microsoft Entra ID or Microsoft Entra hybrid joined VDAs can be enrolled in Intune for enhanced security and application management. Microsoft Intune provides more information regarding Intune enrollment.

Citrix DaaS Flex requires a minimum of VDA Version 2603 or higher for Intune Enrollment, which is supported only for single-session persistent Windows 11 VDAs and not for multi-session VDAs.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

User authentication

Citrix DaaS Flex integrates with the user identity configured in Citrix Cloud. Identity providers provides a complete list of supported identity providers.

If using an identity provider other than Active Directory or Microsoft Entra, Federated Authentication Service (FAS) is required to provide seamless single sign-on to the VDAs.

Access

Citrix DaaS Flex VDAs can be accessed through two primary methods:

- Citrix Workspace
- On-premises Citrix StoreFront

Each of these access layers can be integrated with either an on-premises Citrix Gateway or the cloud-based Citrix Gateway service for secure remote connections. Key differences include:

- Citrix Workspace: Provides the simplicity and ease of management inherent in a cloud service, offering a modern, unified user experience.
- On-premises Citrix StoreFront: Delivers extensive customization options, allowing you to tailor the user interface and overall solution to meet specific branding and functional requirements.

Both platforms offer robust mechanisms for business continuity:

- Workspace with Gateway Service: Features built-in Service Continuity, ensuring users can maintain access to their apps and desktops even during a cloud service or connectivity disruption.
- StoreFront: Utilizes Local Host Cache (LHC), which enables users to continue accessing resources if the on-premises deployment loses its connection to the Citrix Cloud control plane.

Management interfaces

Citrix DaaS Flex for Azure has two graphical management interfaces:

- Quick Deploy
- Web Studio

Quick Deploy: For Citrix DaaS Flex deployments, Quick Deploy serves as the primary management interface. You can access it by navigating to **Quick Deploy > Microsoft Azure** within the Citrix DaaS console.

Web Studio: The DaaS Web Studio configuration interface is the main DaaS management interface. While most catalog creation and management activities must be done through the Quick Deploy interface, some additional capabilities are offered through the Web Studio interface.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Refer to the Differences between Quick Deploy and Studio workflows for more details on use cases for Studio interface (for example: bulk maintenance mode).

When you create a catalog in Quick Deploy, an associated machine catalog, delivery group, and host connection are created automatically in the DaaS Studio.

Manage catalogs created in the Quick Deploy interface

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

Machine catalogs, delivery groups, and connections with the Citrix managed object scope are prohibited from certain actions in the Studio interface. In the Studio interface:

- Delivery group: Most of the delivery group management actions are available, however you cannot delete the delivery group.
- Machine catalog: Operations are locked down and only few are available like power actions and maintenance mode.
- Hosting connection: Operations are locked down and only few are available like power actions and `Set-HypHypervisorConnectionMetadata`. You cannot create a connection that is based on a connection that has the Citrix managed object scope.

When you're ready, get started.

What's new

October 13, 2026

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

October 2026

New and enhanced features

Granular delegated administration for Quick Deploy Citrix DaaS Flex now supports granular delegated administration for Quick Deploy, giving you precise control over what each administrator can

© 1997–2026 Citrix Systems, Inc. All rights reserved.

do. Previously, access was all-or-nothing: only a Cloud Administrator or a Quick Deploy Administrator could manage resources, and each had full control over every catalog, image, network connection, and subscription in the account. There was no read-only option and no way to delegate a subset of functions.

With this release, you can now:

- Grant read-only access so an administrator can view Quick Deploy resources without making changes.
- Create custom roles that allow only a specific subset of Quick Deploy management functions.

The Quick Deploy console adapts to each administrator, showing only the actions they are permitted to perform.

For details, see Custom role and granular permissions in Quick Deploy.

September 2026

New and enhanced features

Time-based access control for Bastion and Image Builder connections Citrix DaaS Flex now supports time-based access control for all RDP, Bastion, and Image Builder connections to Virtual Delivery Agents (VDAs). When an administrator initiates a session through the DaaS Flex Quick Deploy, the system creates the necessary Azure firewall rules and routes to allow RDP traffic through the VNet peering infrastructure. The system automatically removes these rules and shuts down the machines when the specified time window expires, even if an active RDP, Bastion, or Image Builder connection is in progress.

For more information, see Troubleshoot.

Enhanced network connectivity for Pure Entra ID environments Citrix DaaS Flex now offers enhanced network connectivity for environments using Pure Entra ID. You can now seamlessly connect your Entra-joined VDAs to on-premises resources like file shares and legacy applications by leveraging VNet peering, VPN Gateway, and Virtual WAN hub options directly within the machine catalog workflow. This update removes the previous “no connectivity”limitation for Pure Entra ID configurations.

Modify the Active Directory OU path for new machines Citrix DaaS Flex now enables administrators to modify an Active Directory Organizational Unit (OU) path for the following:

- New VDAs added to existing catalogs
- Additional Cloud Connectors added to an existing Resource Location
- Image Builder machines

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Service Account support for machine catalogs Citrix DaaS Flex now allows an administrator to leverage Service Accounts within Citrix DaaS Flex machine catalogs. This integration eliminates the need to manually provide Active Directory domain user or service account credentials during provisioning, troubleshooting, or updating catalog workflows.

July 2026

New and enhanced features

Manage unique user capacity in a catalog Citrix DaaS Flex simplifies user capacity management by allowing administrators to easily scale unique user limits up or down within an existing machine catalog. Simply enter the desired change in unique user count, and Citrix automatically provisions or decommissions machines based on your catalog's established persona. Additionally, you can now select and delete multiple unique machines simultaneously to streamline administrative workflows.

For more information, see Manage user capacity in a catalog.

Multiple IPv4 CIDR ranges for RDP access restrictions Citrix DaaS Flex now supports specifying multiple IPv4 Classless Inter-Domain Routing (CIDR) address ranges when configuring Remote Desktop Protocol (RDP) access restrictions for network connections. Previously, administrators could define only a single IP range. This update removes that limitation across all RDP-based connectivity options, including virtual network (VNet) peering, Bastion host, and other RDP connections, enabling more granular control over permitted source addresses.

For more information, see Troubleshoot.

Time-based access control for RDP connections Citrix DaaS Flex now supports time-based access control for RDP connections to Virtual Delivery Agents (VDAs). When an administrator initiates an RDP session through the DaaS Flex troubleshooting section, the system creates the necessary Azure firewall rules and routes to allow RDP traffic through the VNet peering infrastructure. These rules are automatically removed when the specified time window expires, regardless of whether an active RDP connection is in progress.

For more information, see Troubleshoot.

LTSR version for Citrix prepared images Citrix prepared images now include a Long Term Service Release (LTSR) version alongside the existing Current Release (CU) version of the Citrix Virtual Delivery Agent (VDA) software.

For more information, see Images.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Service endpoints This feature enables the configuration of Service endpoints on Flex VDA subnets through the Admin UI and API. By doing so, we enable secure, direct traffic routing over the Azure backbone, allowing customers to whitelist Flex subnets in their Storage Firewalls.

For more information, see Service endpoints.

Azure Network contributor permission for VNet peering The enhancement allows a customer to enter service principal details for an Azure Network contributor that has fewer permissions than a subscription owner for VNet peering. This aligns with customers'security and compliance requirements.

For more details, see Virtual network peering.

June 2026

New and enhanced features

Manage IPv4 address ranges for an Azure Virtual WAN spoke connection After creating an Azure Virtual WAN spoke connection, you can expand the allocated network space by adding more IPv4 address ranges to the Citrix-managed spoke virtual network. This capability is useful when your existing address range is running low on available IP addresses or when you need to support additional Flex workloads.

For more information, see Manage IPv4 address ranges for an Azure Virtual WAN spoke connection.

Microsoft Entra ID and Intune support Citrix DaaS Flex integrates with Microsoft Entra ID and Intune to strengthen security, meet compliance requirements, and deliver a seamless end-user experience. Combining this functionality with Microsoft Entra Single Sign-on further simplifies user access.

For more information, see Configuring Microsoft Entra ID.

May 2026

New and enhanced features

Initial release of Citrix DaaS Flex Citrix DaaS Flex is a component of Citrix Platform Flex and is a persona-based DaaS service delivered through Citrix Cloud. It enables organizations to deploy and operate virtual apps and desktops without managing the underlying cloud infrastructure. In this release, the Citrix DaaS Flex is applicable only to Azure environments. For more information, see Citrix DaaS Flex for Azure.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Limits

May 11, 2026

This article lists the limits for resources in a Citrix DaaS Flex for Azure deployment.

Configuration limits

Resource	Limit
Active Directory domains	25
Catalogs	100
Resource locations	25
VDAs per subscription	5,000

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
Max Single-session Personas	5,000
Max Multi-session Personas	25,000

Usage limits

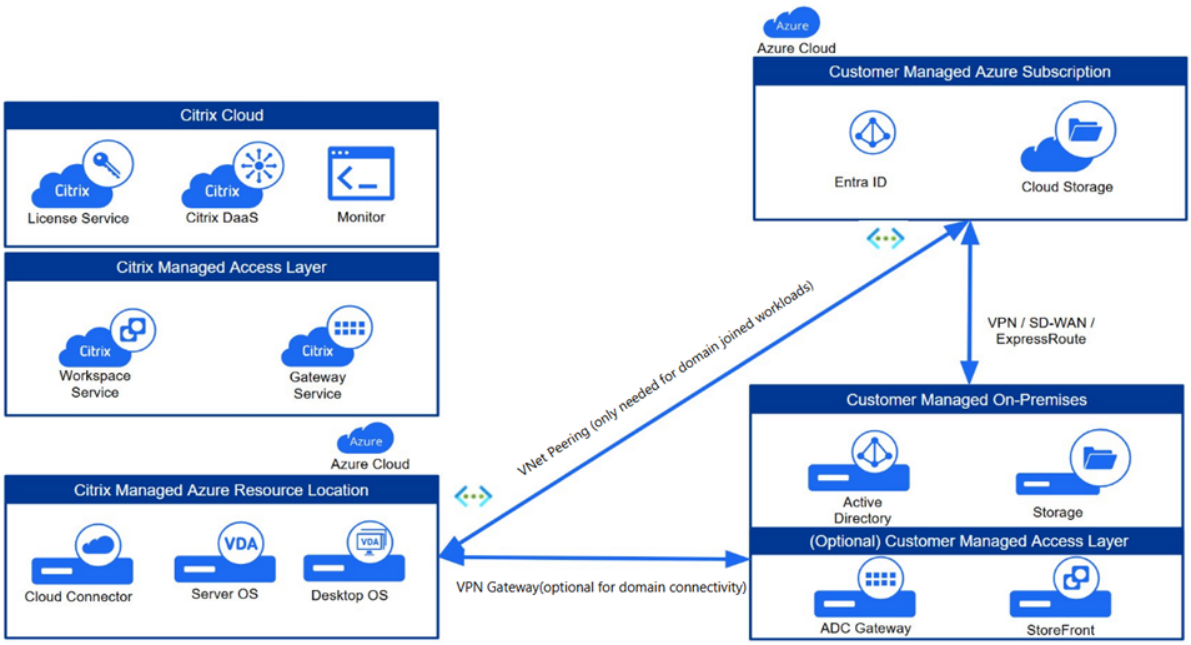
For more information regarding DaaS usage limits, see Limits.

Technical security overview

May 18, 2026

© 1997–2026 Citrix Systems, Inc. All rights reserved.

The following diagram shows the components in a Citrix DaaS Flex deployment. This example uses a virtual network peering connection.



With Citrix DaaS Flex, 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 is responsible for the security of the Azure subscription and Microsoft Entra that are created for your environment. Citrix ensures tenant isolation, so each customer has their own Azure subscription, and cross-talk between different tenants is prevented.

Governance, risk, and compliance

Citrix maintains a comprehensive security program designed to meet the stringent requirements of global enterprises. For a list of Citrix information security and other certifications, see Citrix Trust Center.

- **SOC 2 Type 2**: Processes are independently audited to validate that effective security controls are in place.
- **ISO/IEC 27001**: Validates that data is managed and protected in accordance with international information security standards.
- **ISO/IEC 27701**: Builds on 27001 certification to validate the management of privacy and the processing of Personally Identifiable Information (PII).

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- **Health Insurance Portability and Accountability Act (HIPAA)**: Supports the customer implementation of the technical safeguards required by the HIPAA Security Rule for protecting ePHI.
- **Payment Card Industry Data Security Standard (PCI DSS)**: Supports the customer implementation of the technical safeguards required by PCI DSS.

Customer data is stored within the customer-selected Azure region. Compute, storage, and data processing of workloads deployed through Citrix DaaS Flex remain within the chosen geography to help customers meet their data sovereignty requirements.

Regions

Geography/continent	Available regions
North America (US)	Central US; East US; North Central US; South Central US; West US; West US 2; West US 3
South America	Brazil South
Europe	Germany West Central; Italy North; North Europe; Sweden Central; UK South; West Europe
Asia	Central India; Japan East; Southeast Asia
Australia / Oceania	Australia East

Identity and Access Management (IAM)

Secure access is managed through robust identity controls for both customer Citrix administrators.

- **Citrix Administrative Access**: Access to your subscription is restricted to specific Citrix personnel based on the job function and operational responsibilities. Strict internal security policies govern the use of this access. Citrix personnel cannot access VDAs in a customer-managed subscription.

Network architecture

Citrix-managed virtual network Citrix designs the network architecture for strict tenant isolation and secure connectivity. Virtual networks are created for isolating resource locations within your Citrix-managed Azure subscription. Within those networks, Citrix creates the VDAs, Cloud Connectors, image builder machines, storage accounts, key vaults, and other Azure resources.

Citrix configures the default Azure network security groups to limit access to network interfaces in virtual network peering connections. Generally, this controls incoming traffic to VDAs and Cloud Connectors. Customers cannot change this default firewall policy, but might deploy additional firewall

© 1997–2026 Citrix Systems, Inc. All rights reserved.

rules on Citrix-created VDAs, for example, to partially restrict outgoing traffic. Customers who 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.

For more information regarding firewall policies, see Firewall policy for Citrix DaaS Flex.

Azure virtual network peering For VDAs in a Citrix-managed Azure subscription to contact on-premises domain controllers, file shares, or other intranet resources, a virtual network peering connection can be implemented. The customer's Citrix-managed virtual network is peered with a customer-managed Azure virtual network. The customer-managed virtual network might 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's responsibility for virtual network peering is limited to supporting the peering workflow and related Azure resource configuration for establishing a peering relationship between Citrix and customer-managed virtual networks.

Resiliency

The Citrix DaaS Flex solution is designed in accordance with Citrix leading practices for high availability and resiliency.

- **Availability zones**: Citrix distributes Cloud Connectors and VDAs across availability zones if offered by the Azure region to protect against localized data center failures.
- **Backup VM SKUs**: Citrix designates backup Azure VM SKUs to protect against issues in which capacity is unavailable for the VM SKU of the catalog. If the SKU of the catalog is unavailable due to capacity constraints, the service automatically falls back to a secondary VM SKU.
- **Local Host Cache and Service Continuity**: Citrix has resiliency solutions that can provide end-user access to applications and desktops if Cloud Connectors lose connectivity with Citrix Cloud due to an outage or network communication issue.
- **Disaster Recovery**: In the event of Azure data loss, Citrix recovers as many resources in the Citrix-managed Azure subscription as possible. Citrix attempts to recover the Cloud Connectors and VDAs. If Citrix is unable to recover these items, customers are responsible for creating a new catalog. Citrix assumes that machine images are backed up and that customers have backed up their user profiles, allowing the catalog to be rebuilt.
- **Catalog resiliency**: Resiliency differs for different deployment models:
  - **Static (user is assigned to a single VDA)**: If a user's VDA goes down, they must be placed on a new one to recover. Azure provides a 99.5% SLA for single-instance VMs with standard SSDs. The customer can still back up the user profile, but any customizations made to the

© 1997–2026 Citrix Systems, Inc. All rights reserved.

VDA (such as installing programs or configuring Windows) are lost. Administrators can take scheduled or manual snapshots of static machines.

- **Random (user is assigned randomly to a VDA at launch time)**: This catalog type provides high availability by redundancy. If a VDA goes down, no information is lost because the user's profile resides elsewhere.

Customer responsibility

VDAs and images

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

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

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

Virtual network peering

The customer must open all ports specified in the Firewall policy for Citrix DaaS Flex.

When virtual network 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 the 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 virtual network peering.
- Add Azure network security groups and firewalls to the customer's virtual network and on-premises network to block or restrict traffic from the Citrix-managed IP block.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- 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.

Proxy

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

- Configuring the proxy settings on the VDA machine image or, if the VDA is joined to a domain, using Active Directory Group Policy.
- Maintenance and security of the proxy.
- Proxies are not allowed for use with Citrix Cloud Connectors or other Citrix-managed infrastructure.

Identity and access management (IAM)

Secure access is managed through robust identity controls for both customer end-users.

- **Customer Identity**: Citrix DaaS Flex seamlessly integrates with the identity provider (IdP) configured for Citrix Cloud. See Identity and access management to learn more.
  - For IdPs other than Active Directory, you can enable seamless Single Sign-On (SSO) to VDAs by Enabling single sign-on for workspaces with Citrix Federated Authentication Service (FAS).
  - Citrix Cloud provides Conditional Authentication and Device Posture capabilities to enhance the security posture of your environment.

Citrix and customer shared responsibilities

Citrix Cloud Connector for domain-joined catalogs

Citrix DaaS Flex deploys Cloud Connectors in each resource location. Some catalogs might share a resource location if they are in the same region, virtual network 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

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Customers don't always have access to the Cloud Connectors. However, they might 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 the 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.

Troubleshooting

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, any issues that occur are the responsibility of the customer.

Citrix does not create bastions in the customer's Citrix-managed virtual network within the customer's Citrix-managed subscription. The customer is responsible for creating bastions to diagnose and repair issues. 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.

Bastion host The customer is responsible for providing a strong password used for the local Windows account on the bastion machine. The customer is also responsible for providing an external IP address range that allows RDP access to the bastion. The customer is also responsible for deleting the bastion after troubleshooting is complete. Citrix automatically shuts down the machine and closes the port 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 three 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 virtual network peering is functional, the customer can enable RDP access from their peered virtual network to their Citrix-managed virtual network. If the customer uses this option, they are responsible for accessing the VDAs and Cloud Connectors over the virtual network peer. Source IP address ranges can be specified so RDP access can be restricted further, even within the customer's internal network. The customer needs to use

© 1997–2026 Citrix Systems, Inc. All rights reserved.

domain credentials to log in to these machines. Citrix recommends that customers disable RDP access once issues are resolved to improve the security posture of the environment.

Domain credentials

If the customer elects to use a domain-joined catalog, the customer is responsible for providing 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 must be created specifically for Citrix DaaS Flex to facilitate easy auditing of its usage.
- Scoped: The account requires only permissions to join machines to a domain. It must not be a full domain administrator.
- Secure: A strong password must 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 DaaS Flex subscription. The account is retrieved only if an operation requires the domain account password.

More information

For related information, see:

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

Firewall policy for Citrix DaaS Flex

May 11, 2026

Citrix opens or closes the following ports for inbound and outbound traffic.

Citrix-managed virtual network with non-domain-joined machines

- Citrix specifies the IP range: The managed VNet contains a single subnet with the whole range. Connectors and VDAs are placed into the subnet together and traffic is segregated using service tags.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- Inbound rules
  - Deny all inbound: This includes intra-virtual network traffic from VDA to VDA.
- Outbound rules
  - Allow all traffic outbound.

Citrix-managed virtual network with domain-joined machines

- The customer specifies the IP range. The managed VNet contains a single subnet with the whole range. Connectors and VDAs are placed into the subnet together and traffic is segregated using service tags.
- Inbound rules:
  - Allow ports 80, 443, 1494, and 2598 inbound internally to the VDAs and Connectors.
  - Allow ports 49152-65535 inbound to the VDAs from customer's network connection used by the Monitor shadowing feature. See Communications Ports Used by Citrix Technologies.
  - Deny all other inbound.
- Outbound rules
  - Allow all traffic outbound.
  - Can be modified using custom routes.

Customer-managed virtual network with domain-joined machines

- It is up to the customer to configure their virtual network 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 virtual network (IP range specified by customer) to the domain controller, DNS server, and so on.
  - Allow inbound on ports opened with a proxy configuration.
  - Other rules created by the customer.
- Outbound rules:
  - Allow outbound on 443, 1494, 2598 to the Citrix virtual network (IP range specified by customer) for internal launches.
  - Other rules created by the customer.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Firewall policy when using the image builder or troubleshooting tools

When a customer uses the image builder or requests the creation of a bastion machine for troubleshooting, the following security group modifications are made to the Citrix-managed virtual network:

- Temporarily allow 3389 inbound from the customer-specified IP range to the image builder VM or bastion.
- If using a bastion machine, temporarily allow 3389 inbound from the bastion IP address to any address in the virtual network (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 virtual network:

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

Get started

June 23, 2026

This article summarizes the prerequisites that must be met to begin delivering apps and desktops through Citrix DaaS Flex.

Authentication

To authenticate users with your own Identity Provider (IDP), you must first configure it in Citrix Cloud. For detailed instructions, see the documentation on Identity and Access Management.

For IdPs other than Active Directory, you can enable seamless Single Sign-On (SSO) to VDAs by implementing the Citrix Federated Authentication Service (FAS). Enable single sign-on for workspaces with Citrix Federated Authentication Service provides additional details regarding FAS.

Networking

Before creating a catalog, you should consider the network connectivity requirements of your VDAs. If the VDA has requirements to be domain-joined or needs to access resources or files on an internal

© 1997–2026 Citrix Systems, Inc. All rights reserved.

network, connectivity between the Citrix-managed Azure subscription and your resources must be established. The following connectivity options are available:

- **Virtual network peering**: Virtual network peering leverages the Azure backbone to provide a low-latency connection between the Citrix-managed Azure virtual network and a virtual network in your Azure subscription. Further connectivity to resources outside of Azure can be established by connecting the virtual network to your other networks through an Azure ExpressRoute, VPN Gateway, or similar connectivity options.
- **VPN Gateway**: Azure VPN Gateways can be used to connect the Citrix-managed Azure virtual network directly to an on-premises network over the public internet. It can be used to bypass the middle-hop of a virtual network peer.
- **Virtual WAN peering**: An Azure Virtual WAN spoke connection provides direct network connectivity between the Citrix-managed Azure virtual network and your corporate network by connecting the Citrix-managed network as a spoke to an Azure Virtual Hub that you control.
- **No connectivity**: For deployments in which VDAs don't need connectivity to your other networks, you can create a resource location that lacks connectivity to your networks. Only non-domain-joined and Entra ID VDAs are supported in resource locations without connectivity.

For environments with virtual network peering or VPN Gateway connectivity, to enhance the security posture of your environment, you might want to route all outbound traffic from your VDAs through a security appliance in your network. This can be achieved through a custom, or user-defined, route in Azure. Custom routes override Azure's default system routes for directing traffic between virtual machines in a virtual network peering, on-premises networks, and the Internet.

Images

Before you can create a machine catalog in Citrix DaaS Flex, you must first have an image imported to the service. This image acts as the template from which all the virtual machines (VDAs) in your catalog are cloned. Every machine created within the catalog is a direct copy of this master image, ensuring that each one has the same operating system, applications, and initial configuration.

You have three primary options for sourcing this master image.

- The simplest method is to use one of the Citrix-prepared images, which are pre-built and optimized with the necessary Citrix components already installed.
- For more specific needs, you can build a custom image by taking a Citrix-prepared image, adding your own applications and configurations, and then saving it as a new template.
- Finally, if you already have a standardized image in your own Azure subscription, you have the option to import your own image provided it has been properly prepared with the required Citrix VDA software.

To learn more about importing and configuring images, see Images.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Access

Citrix DaaS Flex VDAs can be accessed through two primary methods:

- Citrix Workspace
- On-premises Citrix StoreFront

Workspace

If using the cloud-hosted Citrix Workspace service, you must first configure the service. See Get started with Citrix Workspace for more information on configuring Citrix Workspace.

To enhance environment resiliency, it is highly recommended to enable Service Continuity if using Citrix Workspace for end-user access.

StoreFront

If using a customer-managed StoreFront access method, you must build a StoreFront and NetScaler Gateway deployment in your environment. See Get started for more information on planning and building a StoreFront deployment.

The StoreFront deployment must have connectivity to the Cloud Connectors hosted in the Citrix-managed Azure subscription and must be listed in the DaaS site in StoreFront. The inbound ports in the Citrix-managed virtual network are blocked by default. Contact Citrix support to get them opened. If connectors are not listed in the site or the connectors are unreachable from the StoreFront server, resources might be unavailable if your site transitions into Local Host Cache (LHC) mode.

Azure subscriptions

May 11, 2026

A Citrix DaaS Flex subscription supports the number of VDAs indicated in Limits.

If your Citrix DaaS Flex subscription is likely to reach its limit soon, and you have enough Citrix licenses, you can request another Citrix DaaS Flex subscription. The **Quick Deploy** contains a notification when you're close to the limit.

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

For example, assume a hypothetical limit of 5,000 machines per Citrix DaaS Flex subscription.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- Let's say you have two catalogs ('Cat1'and 'Cat2') that use the same Citrix DaaS Flex subscription. 'Cat1'currently contains 2,000 machines, and 'Cat2'has 1,500.
- As you plan for future capacity needs, you add 1,000 machines to 'Cat2'. The Citrix DaaS Flex subscription now supports 4,500 machines (2,000 in 'Cat1'and 2,500 in 'Cat2'). The dashboard indicates that the subscription is near its limit.
- When you need 500 more machines, you can't use that subscription to create a catalog with 500 machines (or add 500 machines to an existing catalog). That would exceed the subscription limit. Instead, you request another Citrix DaaS Flex subscription. Then, you can create a catalog using that subscription.

When you have more than one Citrix DaaS Flex subscription:

- Nothing is shared between those subscriptions.
- Each subscription has a unique name.
- You can choose among the Citrix DaaS Flex subscriptions when:
  - Creating a catalog
  - Building or importing an image
  - Creating a VNet peering or Azure VPN gateway connection.

Add a Citrix DaaS Flex subscription

1. Contact your Citrix representative to request another Citrix DaaS Flex subscription. You are notified when you can proceed.
2. From the Citrix DaaS Flex dashboard, expand **Cloud Subscriptions**.
3. Click **Add Azure subscription**.
4. On the **Add Subscriptions** page, click **Add a Citrix DaaS Flex 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 DaaS Flex subscription, contact Citrix Support.

Remove a Citrix DaaS Flex subscription

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

> **Note:**
>
> You can't remove all Citrix DaaS Flex subscriptions. At least one subscription must remain in the tenant.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

1. From the Citrix DaaS Flex dashboard, expand **Cloud Subscriptions**.
2. Select the subscription you plan to delete.
3. On the **Details** tab, click **Remove Subscription**.
4. Click **Authenticate Azure Account** and log in to the Azure log in page.
5. You're returned automatically to the Citrix DaaS Flex console. Confirm the deletion in the check boxes and then click **Yes, Delete Subscription**.

Network connections

July 30, 2026

Introduction

When creating a catalog, you indicate if and how users access locations and resources on their corporate on-premises network from their Citrix DaaS Flex VDAs.

When using a Citrix DaaS Flex subscription, the available options are:

- No connectivity
- Virtual network peering
- Azure VPN Gateway
- Virtual vWAN Peering

> **Note:**
>
> You cannot change a catalog's connection type after the catalog is created.

No connectivity

When a catalog is configured with **No connectivity**, users cannot access resources on their on-premises or other networks. Only non-domain-joined and Entra ID deployments are supported for VDAs in a resource location with no connectivity.

Requirements for all network connectivity methods

- When creating a connection, you must have valid DNS server entries.
- When using Secure DNS or a third-party DNS provider, you must add the address range that is allocated for use by Citrix DaaS Flex to the DNS provider's IP addresses on the allow list. That address range is specified when you create a connection.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- All service resources that use the connection (domain-joined machines) must be able to reach your Network Time Protocol (NTP) server to ensure time synchronization.

Virtual network peering

To facilitate VDA access to resources within your corporate network, establish a virtual network peering connection between the Citrix-managed Azure subscription and your own. This configuration is required for domain-joined VDAs or for those requiring access to services in your Azure subscription or on-premises data center.

To extend access from VDAs to resources in your on-premises data center, a further connection is required from your Azure subscription to the on-premises data center. This can be achieved through an Azure ExpressRoute or VPN. Connectivity between customer-managed subscriptions and on-premise data centers is outside of the scope of Citrix DaaS Flex and is managed by the customer.

> **Important:**
>
> A virtual network peer must be created before creating a catalog that uses it.

Requirements for configuring a virtual network peer

- A customer-managed Azure subscription, resource group, and virtual network.
- Credentials for an Azure Resource Manager subscription owner permissions or service principal of an Azure Network Contributor. The account must be an Azure Active Directory account native to the same Azure AD which is associated with the subscription of the customer-managed virtual network. Citrix DaaS Flex does not support other account types, such as live.com or external (guest) Azure AD accounts in a different tenant.
- Azure network routes in which VDAs in the Citrix-managed Azure subscription can communicate with your network.
- Network Security Group (NSG) rules that allow communication from the IP range of the Citrix DaaS Flex VDAs to your virtual network.
- If you plan for VDAs to be domain-joined, Citrix recommends Active Directory services running in the peered virtual network in your subscription to take advantage of the low latency between the peered virtual networks.
- 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 virtual networks being connected. This is the IP range assigned to the VMs within the Citrix DaaS Flex virtual network. Ensure that you specify an IP range that does not overlap any addresses that you use in your Azure and on-premises networks.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- For example, if your Azure virtual network has an address space of 10.0.0.0 /16, create the virtual network peering connection in Citrix DaaS Flex 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 virtual network peering connection might not be created successfully. It might also cause issues when performing site administration tasks.
- A /24 IP range is the minimum size of a virtual network within the Citrix DaaS Flex tenant.

Azure virtual network peering connection custom routes

To enhance the security posture of your environment, you might want to route all outbound traffic from the VDA through a security appliance in your managed Azure subscription. This can be achieved through a custom, or user-defined, route in Azure. Custom routes override Azure's default system routes for directing traffic between virtual machines in a virtual network peering, on-premises networks, and the Internet.

To use custom routes:

- You must have an existing Azure VPN gateway or a network appliance in your Citrix DaaS Flex environment.
- When you add custom routes, you must update your company's route tables with the Citrix DaaS Flex destination virtual network information to ensure end-to-end connectivity.
- Custom routes are displayed in Citrix DaaS Managed Azure in the order in which they are entered. This display order does not affect the order in which Azure selects routes.

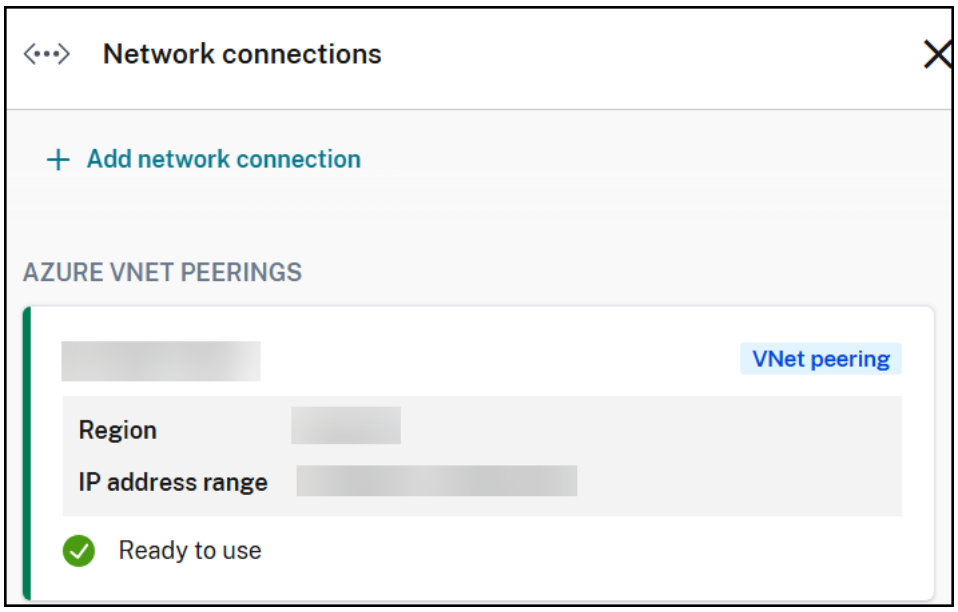
Before using custom routes, review the Microsoft article Virtual network traffic routing to learn about using custom routes, next hop types, and how Azure selects routes for outbound traffic.

You can add custom routes when you create an Azure virtual network peering connection or to existing virtual network peering connections in your Citrix DaaS Flex environment.

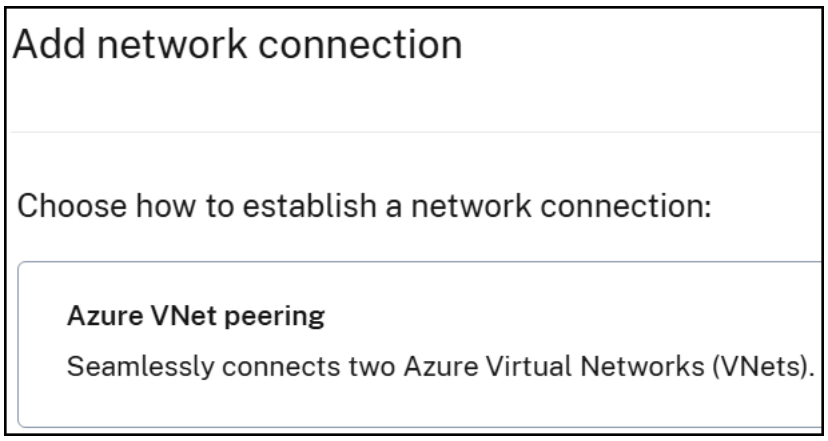
Create an Azure virtual network peering connection

1. From the **Quick Deploy > Microsoft Azure** dashboard, expand **Network connections** on the right.
2. Click **Add network Connection**.

© 1997–2026 Citrix Systems, Inc. All rights reserved.



3. On **Add network Connection** page, click **Azure VNet peering**.

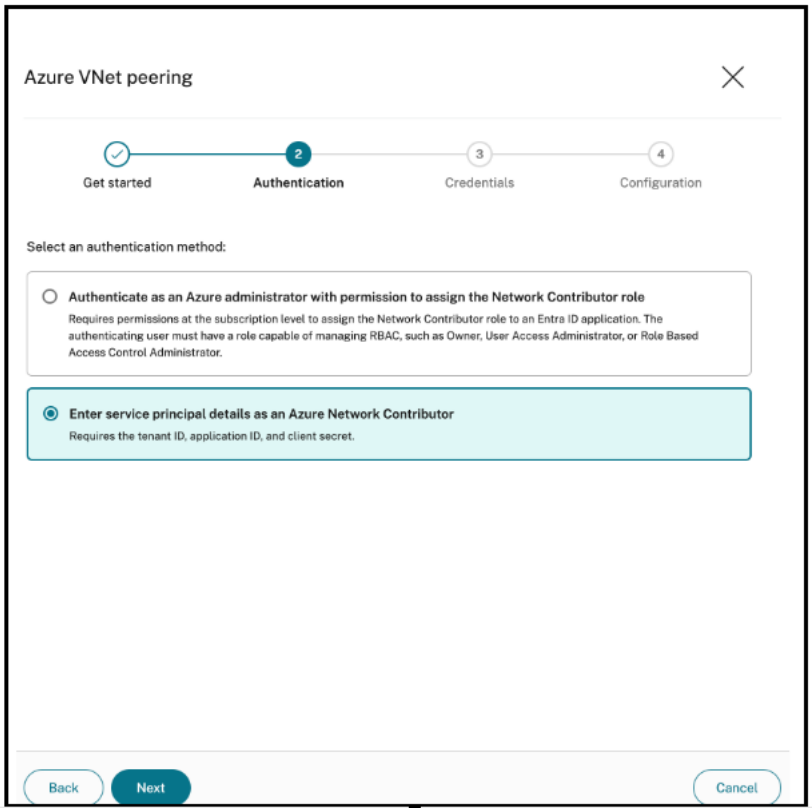


There are two options for creating VNet peering based on role permissions:

- Authenticate as an Azure administrator with permissions at the subscription level.
- Enter service principal details as an Azure Network Contributor.

4. Select the authentication method and click **Next**.

© 1997–2026 Citrix Systems, Inc. All rights reserved.



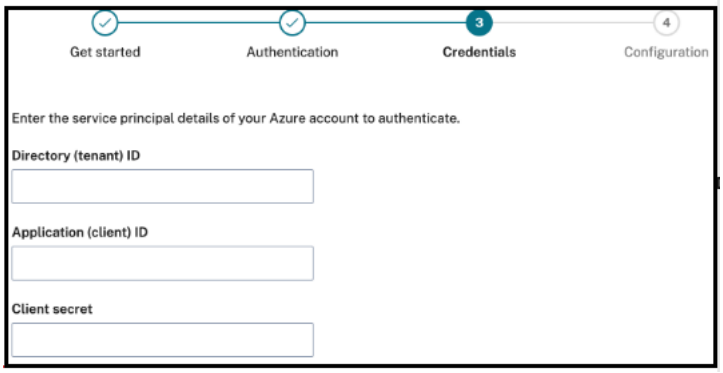
5. If **Authenticate as an Azure administrator** option is selected:

   a) Click **Authenticate Azure Account**.

   b) Citrix DaaS Flex automatically takes you to the Azure sign-in page to authenticate your Azure subscriptions. After you sign in to Azure and accept the terms, you are returned to the connection creation details dialog.

6. If **Enter service principal details as an Azure Network Contributor** option is selected:

   a) Enter Directory ID, Application ID, and Client secret, then click **Next** to authenticate.



7. Once authenticated successfully, on the dialog page:

   a) Type a name for the Azure virtual network peer.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

b) Select the Azure subscription, resource group, and the virtual network to peer with.

c) Indicate whether the selected virtual network uses an Azure Virtual Network Gateway. For information, see the Microsoft article Azure VPN Gateway.

d) If your virtual network uses an Azure Virtual Network Gateway, indicate whether you want to enable virtual network gateway route propagation. When enabled, Azure automatically adds all routes through the gateway.

> **Note:**
>
> You can change this setting later from the connection's **Details** page. However, changing it can cause route pattern changes and VDA traffic interruptions. Also, if you disable it later, you must manually add routes to networks that VDAs use.

e) Type an IP address and select a network mask. The address range to be used is displayed, along with the number of addresses supported by the range. Ensure that the IP range does not overlap any addresses that you use in your Azure and on-premises networks.

f) Indicate whether you want to add custom routes to the virtual network peering connection. If you select **Yes**, enter the following information:

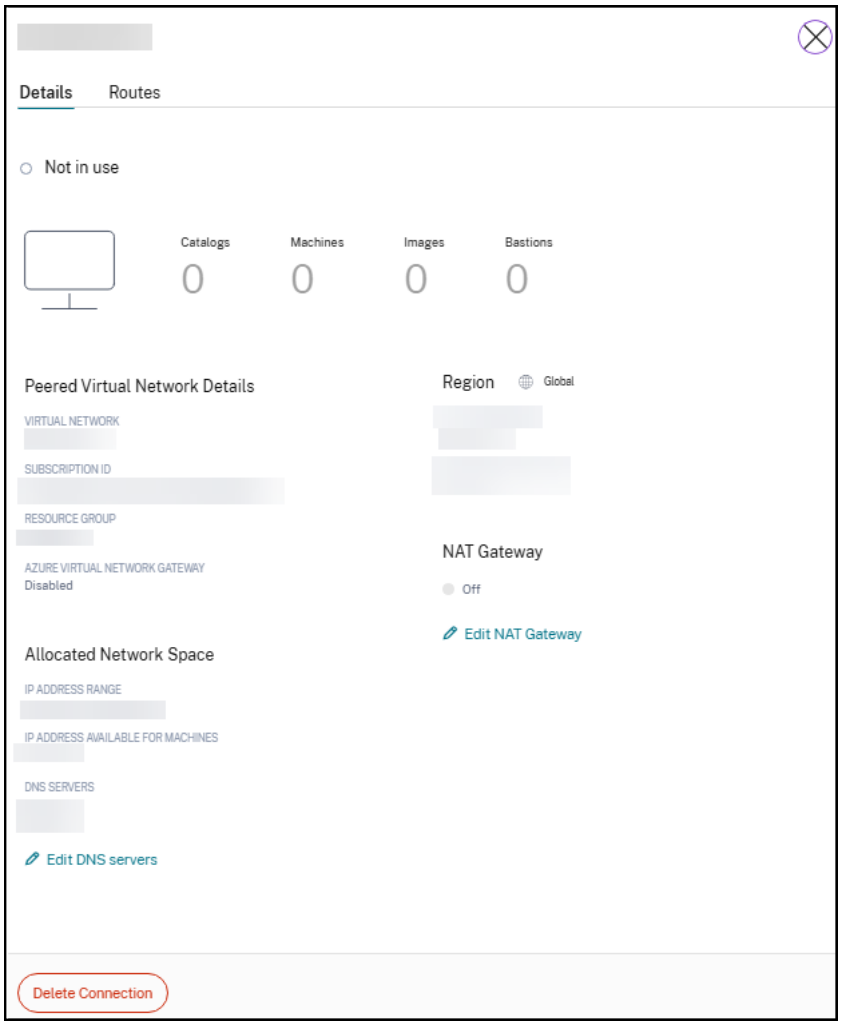
   i. Type a friendly name for the custom route.
   ii. Enter the destination IP address and network prefix. The network prefix must be between 16 and 24.
   iii. Select the next hop type for where you want traffic to be routed. If you select Virtual appliance, enter the internal IP address of the appliance.
   iv. Click **Add route** to create another custom route for the connection.

g) Click **Add VNet Peering** to add the network connection.

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

© 1997–2026 Citrix Systems, Inc. All rights reserved.

View Azure virtual network peering connection details



1. From **Quick Deploy > Microsoft Azure**, expand **Network connections** on the right.
2. Select the Azure virtual network peering connection you want to display.

   The **Details** tab displays:

   - The number of catalogs, machines, images, and bastions that use this connection.
   - The region, allocated network space, and peered virtual networks.

   The **Routes** tab displays:

   - The routes that are currently configured for the virtual network peering connection.

Manage custom routes for existing Azure virtual network peer connections

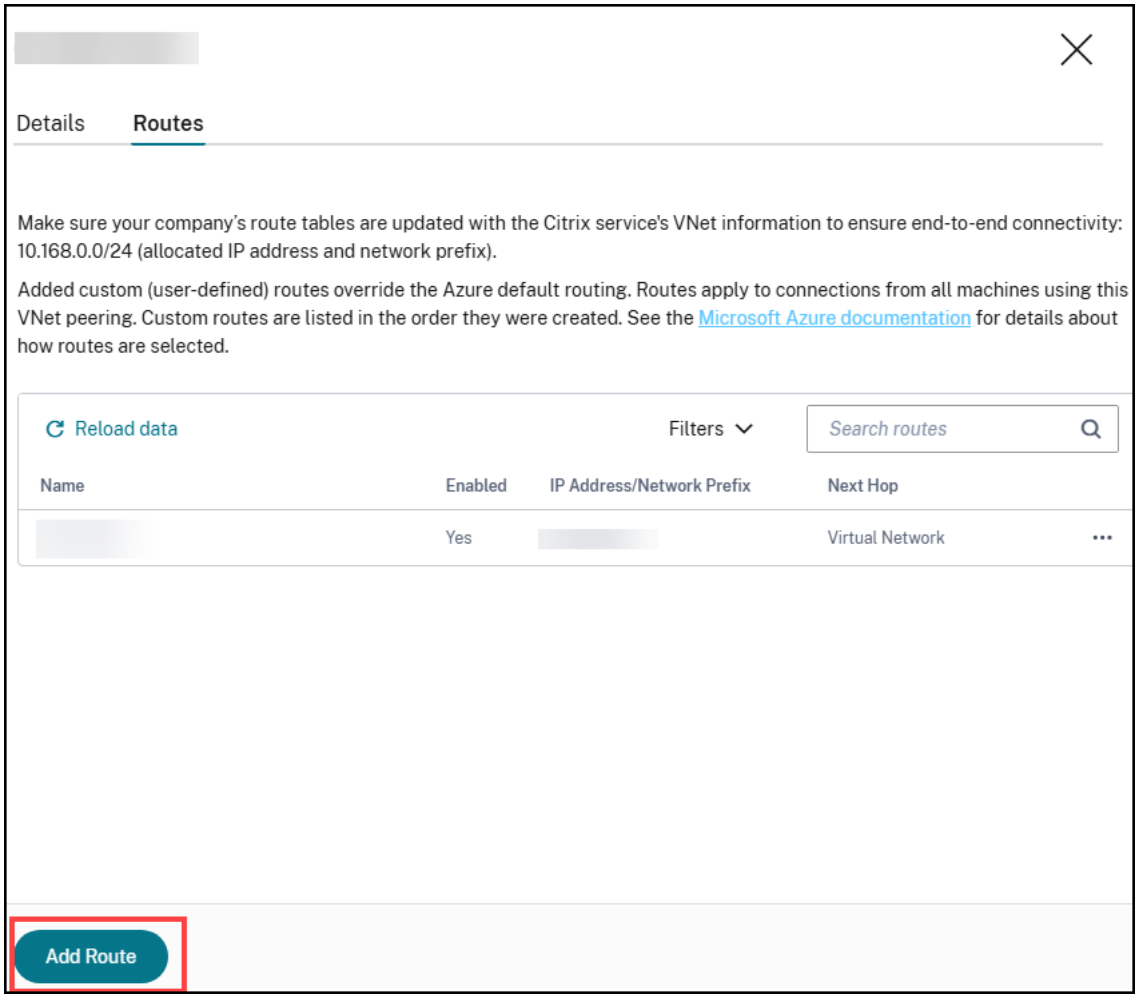
You can add new custom routes to an existing connection or modify existing custom routes, including disabling or deleting custom routes.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

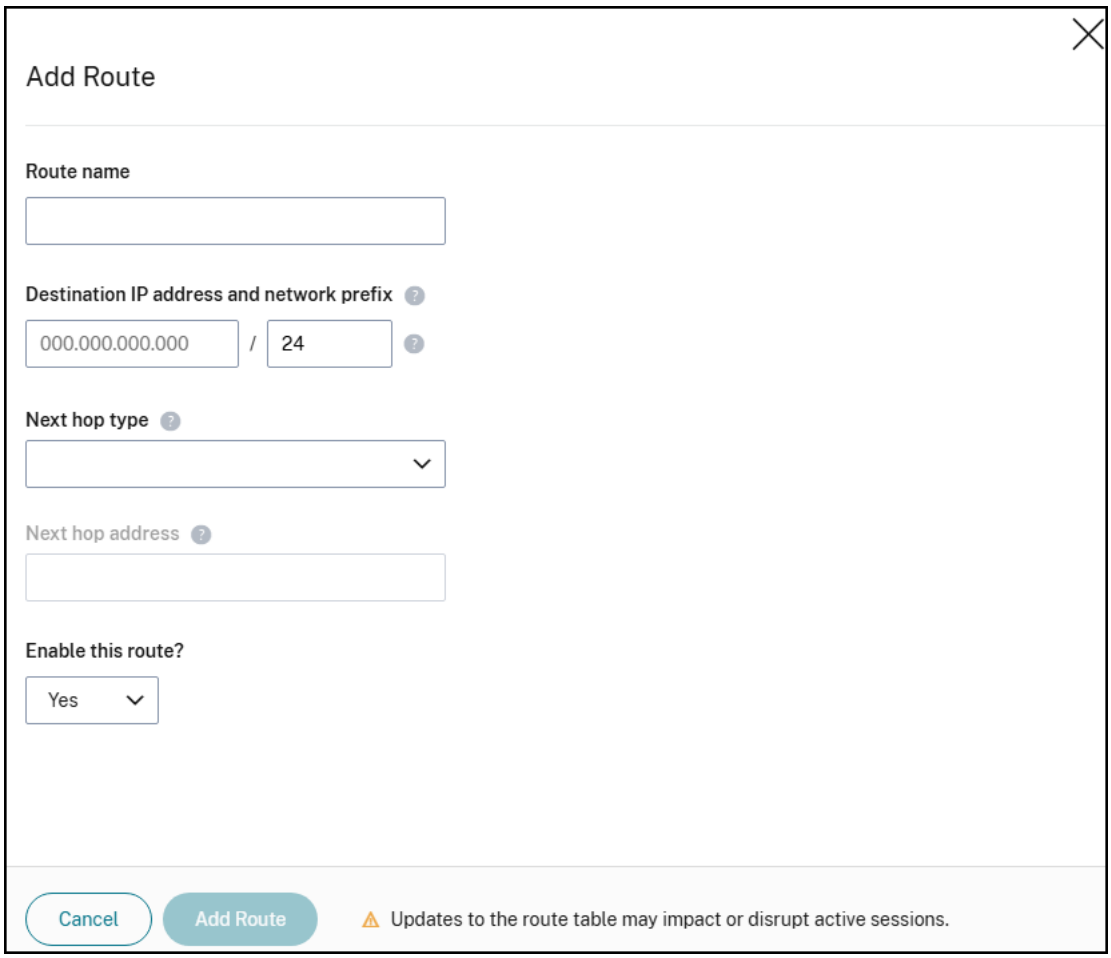
> **Important:**
>
> Modifying, disabling, or deleting custom routes changes the traffic flow of the connection and might disrupt any user sessions that might be active.

Add a custom route

1. From the virtual network peering connection details, click **Routes > Add Route**.



© 1997–2026 Citrix Systems, Inc. All rights reserved.

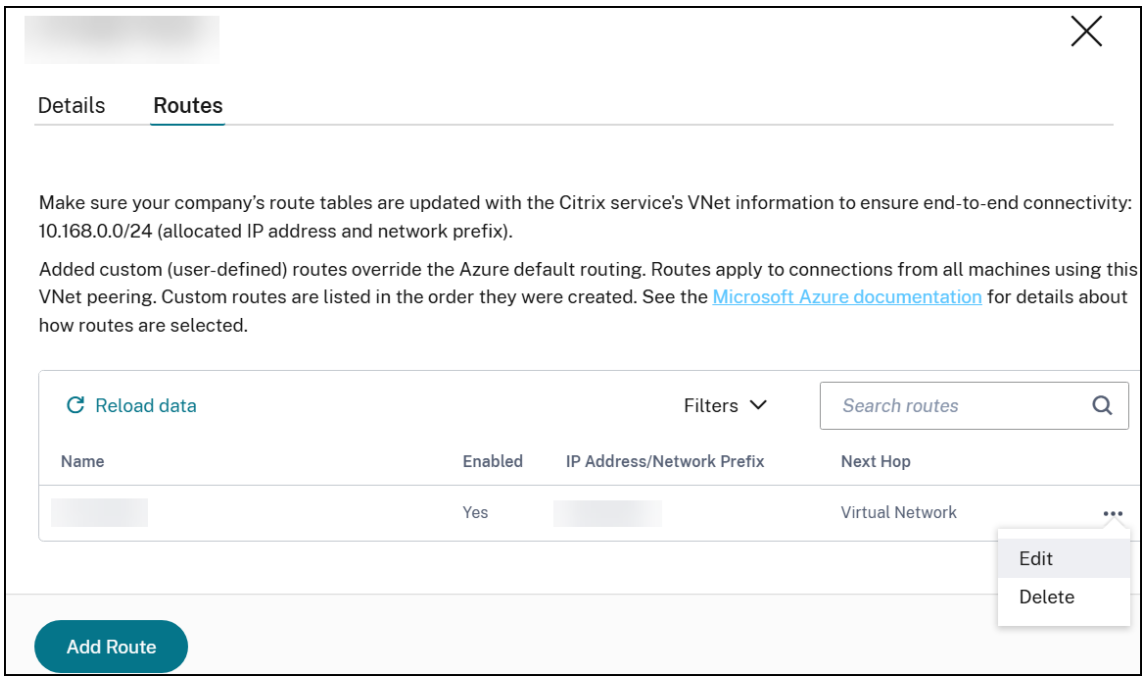


2. Enter a friendly name, the destination IP address and prefix, and the next hop type you want to use. If you select **Virtual Appliance** as the next hop type, enter the internal IP address of the appliance.
3. Indicate whether you want to enable the custom route. By default, the custom route is enabled.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

Modify or disable a custom route

1. From the virtual network peering connection details, select **Routes** and then locate the custom route you want to manage.

© 1997–2026 Citrix Systems, Inc. All rights reserved.



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**.

Delete a custom route

1. From the virtual network 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**.

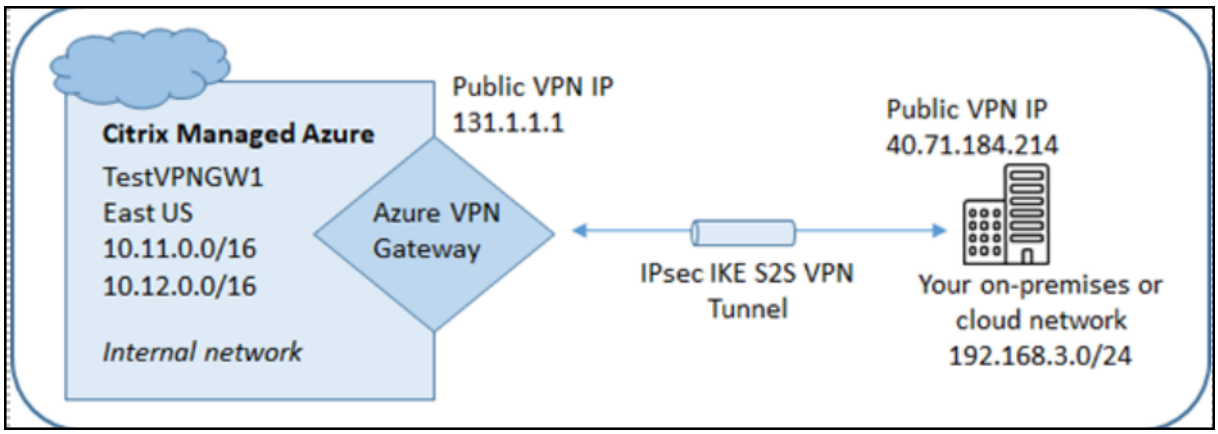
Delete an Azure VNet peering connection Before you can delete an Azure VNet peer, remove any catalogs associated with it. See Delete a catalog for more information on deleting catalogs.

1. From **Quick Deploy > Microsoft Azure**, expand **Network connections** on the right.
2. Select the connection you want to delete.
3. From the connection details, click **Delete Connection**.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Azure VPN gateway

An Azure VPN gateway can be used to provide direct communication between your Citrix-managed Azure VDAs and your on-premises network, without the need of additional hop through a peered Azure virtual network. The secure connectivity uses the industry-standard protocols Internet Protocol Security (IPsec) and Internet Key Exchange (IKE).



During the connection creation process:

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

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

Azure VPN gateway connection requirements and preparation

- To learn about Azure VPN Gateway, see the Microsoft article What is VPN Gateway?
- Review the requirements for all network connections.
- You must have a configured VPN. The virtual network must be able to send and receive traffic through the VPN gateway. A virtual network can't be associated with more than one virtual network gateway. The configured VPN must have:
  - An IPsec device that has a public IP address. To learn about validated VPN devices, see the Microsoft article About VPN devices.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- Additional prerequisites might be required based on your VPN configuration. Read the Create an Azure VPN Gateway connection section entirely before beginning to determine requirements from your VPN appliance.

Azure VPN gateway custom routes

To enhance the security posture of your environment, you might want to route all outbound traffic from the VDA through a security appliance. Custom routes override default system routes for directing traffic between virtual machines in your networks and the Internet.

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

To use custom routes:

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

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

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

Create an Azure VPN Gateway connection

Review the entire section before beginning the process to ensure all prerequisites are met.

1. From the **Quick Deploy > Microsoft Azure** dashboard, expand **Network connections** on the right.
2. Click **Add network Connection**.
3. Click **Azure VPN Gateway**.
4. Review the information on the **Add VPN Connection** page, and then click **Start Configuring VPN**.
5. On **Add a VPN** page, provide the following information.

    a) **Name your connection**: A name for the connection.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

b) **VPN IP address**: The public-facing IP address of the VPN appliance in your network.

c) **Allowed networks**: One or more address ranges that the Citrix service is allowed to access on your network. Usually, this address range contains the resources that your users need to access, such as file servers. To add more than one range, click **Add more IP addresses** and enter a value. Repeat as needed.

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

e) **Performance and throughput**: The bandwidth level to use when your users access resources on your network. Not all choices support Border Gateway Protocol (BGP). In those cases, the BGP settings fields aren't available.

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

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

- Although this address range is maintained in the Citrix-managed Azure subscription, it functions as if it is an extension of your network. The IP range must not overlap any addresses that you use in your on-premises or other cloud networks. If addresses overlap, the connection might not be created successfully. Also, an overlapping address might negatively impact site administration tasks.
- The VDA subnet range must be different from the gateway subnet address.
- You cannot change this value after you create the connection. To use a different value, create another connection.

h) **Gateway subnet**: The address range where the Azure VPN gateway resides when you create a catalog that uses this connection.

- The IP range must not overlap any addresses that you use in your on-premises or other cloud networks. If addresses overlap, the connection might not be created successfully. Also, an overlapping address might negatively impact site administration tasks.
- The gateway subnet range must be different from the VDA subnet address.
- You cannot change this value after you create the connection. To use a different value, create another connection.

i) **Routes**: Indicate whether you want to add custom routes to the connection. If you want to add custom routes, provide the following information:

© 1997–2026 Citrix Systems, Inc. All rights reserved.

i. Type a friendly name for the custom route.
ii. Enter the destination IP address and network prefix. The network prefix must be between 16 and 24.
iii. Select a next hop type for where you want traffic to be routed. If you select **Virtual appliance**, enter the internal IP address of the appliance. For more information about next hop types, see the Microsoft article Custom routes.
iv. To add more than one route, click **Add route** and enter the requested information.

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

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

k) Click **Create VPN connection**.

After Citrix creates the connection, it is listed under **Network Connections > Azure VPN Gateway** in the Quick Deploy dashboard. The connection card contains a public IP address.

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

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

- Update your company's route tables with the Azure VPN gateway connection information to ensure end-to-end connectivity.
- If you configured custom routes, make the appropriate updates for them, too.
- When both ends of the connection are successfully configured, the connection's entry in ***Network Connections > Azure VPN Gateway** indicates **Ready to use**.

View an Azure VPN Gateway connection

1. From the Quick Deploy dashboard, expand **Network connections** on the right.
2. Select the connection you want to display.

   The **Details** tab displays:

   - The number of catalogs, machines, images, and bastions that use this connection. It also contains most of the information you configured for this connection.

   The **Routes** tab lists custom route information for the connection.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Manage custom routes for an Azure VPN gateway connection

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

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

1. From the Azure Quick Deploy dashboard, expand **Network Connections** on the right.
2. Select the connection you want to display.

Add a custom route

1. From the connection's **Routes** tab, 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**.

Modify or enable or disable a custom route

1. From the connection's **Routes** tab, locate the custom route you want to manage.
2. From the ellipsis menu, select **Edit**.
3. Change the destination IP address and prefix, or the next hop type, as needed.
4. Indicate whether you want to enable the route.
5. Click **Save**.

Delete a custom route

1. From the connection's **Routes** tab, 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**.

Reset or delete an Azure VPN gateway connection

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

© 1997–2026 Citrix Systems, Inc. All rights reserved.

> that use it. See Delete a catalog.

To reset or delete a connection:

1. From the Azure Quick Deploy dashboard, expand **Network connections** on the right.
2. Select the connection you want to reset or delete.
3. From the connection's **Details** tab:
   - Click **Reset Connection**, to reset the connection.
   - Click **Delete Connection**, to delete the connection.
4. If prompted, confirm the action.

Create a public static IP address

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

To enable a NAT gateway for a connection:

1. From the Azure Quick Deploy dashboard, expand *Network connections** on the right.
2. Under **Network Connections**, select a connection under **Citrix Managed** or **Azure VNet Peerings**.
3. In the connection details card, click **Enable NAT Gateway**.
4. In the **Enable NAT Gateway** page, move the slider to **Yes** and configure an idle time.
5. Click **Confirm Changes**.

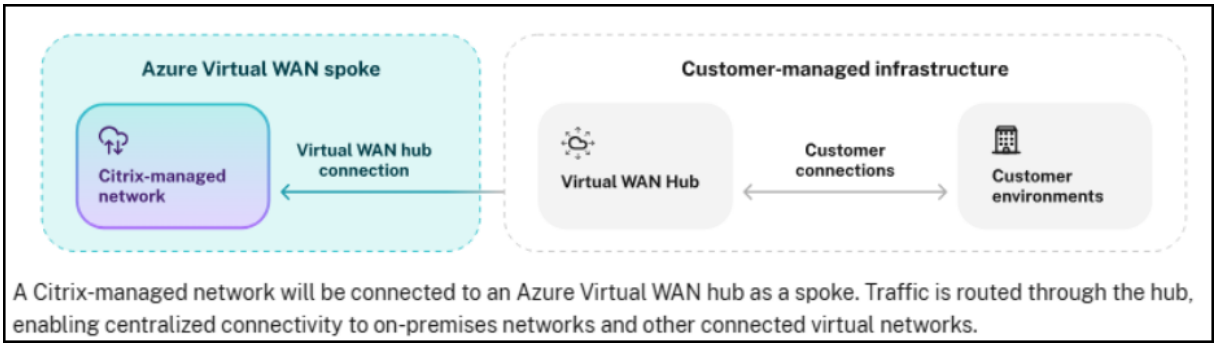
When you enable a NAT gateway:

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

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

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Azure Virtual WAN Peering



A Citrix-managed network will be connected to an Azure Virtual WAN hub as a spoke. Traffic is routed through the hub, enabling centralized connectivity to on-premises networks and other connected virtual networks.

An Azure Virtual WAN spoke connection provides direct network connectivity between the Citrix-managed Azure virtual network and your corporate network by connecting the Citrix-managed network as a spoke to an Azure Virtual Hub that you control. When both your corporate network and the Citrix-managed network are connected to the same Virtual Hub, Citrix infrastructure can reach your on-premises and Azure-hosted resources without requiring a separate peered Azure subscription.

Use this connection type when your organization already uses Azure Virtual WAN for centralized routing across multiple sites, and you want to extend that hub to cover Citrix DaaS Flex VDA traffic.

> **Note:**
>
> Create a Virtual WAN spoke connection before creating a catalog that uses it.

Requirements for configuring an Azure Virtual WAN spoke connection

Before creating the connection, ensure the following conditions are met:

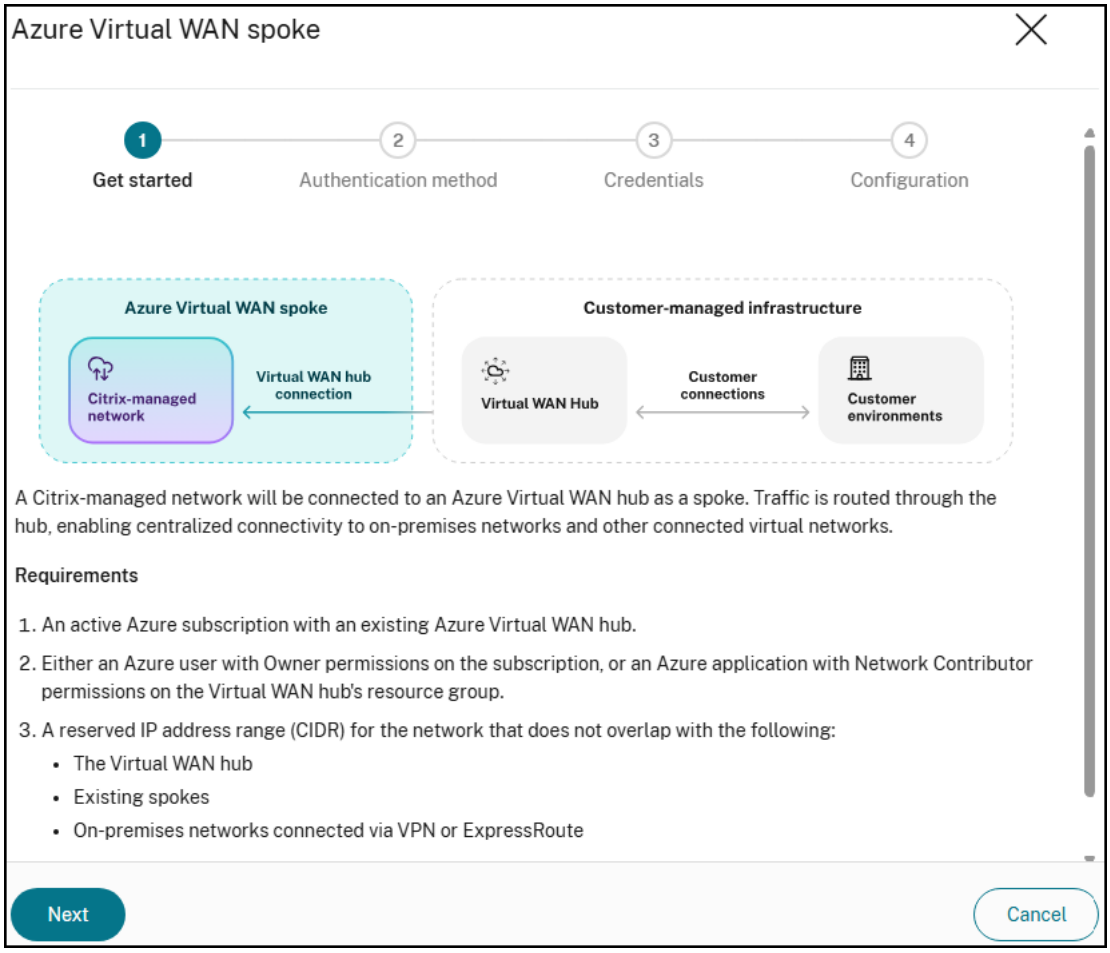
- An Azure subscription containing an existing Azure Virtual WAN and Virtual Hub of type Standard. The Basic tier does not support the VNet connections required for this setup.
- The Virtual Hub Resource ID, resource group, and hub name, available from the hub's Properties page in the Azure portal.
- One of the following:
  - An Azure admin account with Owner permissions on the Virtual Hub resource group (to authenticate through the Citrix UI), or
  - A service principal (app registration) with the Network Contributor role on the Virtual Hub resource group (for automation or least-privilege access).
- An IP address block for Citrix to use for its managed spoke network (for example, 10.200.0.0/24). This range must not overlap with your Virtual Hub address space, or any other network connected to the hub.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- The IP addresses of one or more DNS servers that can resolve your domain name from within Azure.
- Your Citrix customer ID, visible in the Citrix Cloud portal under Identity and Access Management.
- Confirmation that your Citrix DaaS Flex subscription is active. If unsure, contact your Citrix account team.

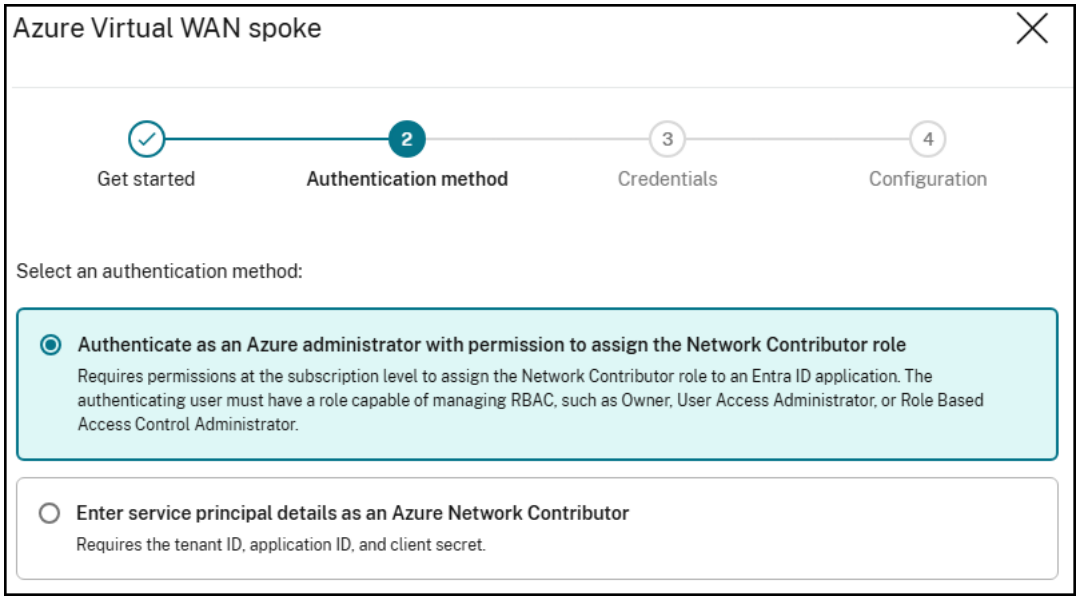
Create an Azure Virtual WAN spoke connection

1. From the **Quick Deploy > Microsoft Azure** dashboard, expand **Network connections** on the right.
2. Click **Add network Connection**.
3. Select **Azure Virtual WAN spoke** as the connection type. Click **Next**.



4. Select an authentication method.

© 1997–2026 Citrix Systems, Inc. All rights reserved.



- **Authenticate as an Azure administrator**: The wizard redirects you to the Azure login page. Sign in with an account that has Owner permissions on the Virtual Hub resource group.
  - Select single-tenant or multi-tenant. Single-tenant is used when the account is in the same Entra tenant as the hub's subscription. Otherwise, use multi-tenant where the subscription tenant ID can be specified.
- **Enter service principal details as an Azure Network Contributor**: Enter the Tenant ID, Application (client) ID, and Client secret for a service principal that has the Network Contributor role on the Virtual Hub resource group.

  To create a service principal with the correct permissions:

  a) In the Azure portal, go to **Microsoft Entra ID > App registrations > New registration**.
  b) After registering, go to **Certificates & secrets** and create a new client secret. Record the value as it is shown only once.
  c) Navigate to the **Virtual Hub resource group**, open Access control (IAM), and assign the Network Contributor role to the app registration.

5. On the **Configuration** page, provide the following:

Field	Value
Network connection name	A name for this connection
Azure subscription	The subscription containing your Virtual Hub
Resource group	The resource group containing your Virtual Hub

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Field	Value
Azure Virtual WAN hub	Select your hub. Must be in a region supported by the Citrix managed subscription
IP address range (CIDR)	The address range for the Citrix managed spoke network (for example, 10.200.0.0/24). Must not overlap with the hub or any connected spoke
DNS servers	IP addresses of DNS servers that can resolve your domain name
Custom routes	Optional. Add a route with destination 0.0.0.0/0 and next hop type Internet to allow Citrix machines to reach the internet for software downloads
Route propagation	Set to **Enabled** to share spoke routes with the hub and connected networks

> **Note:**
>
> You can't change the Advanced settings (Internet security, route propagation) in Citrix Cloud after the connection is created.

6. Click **Add**. The connection appears under **Network connections** with status as **Provisioning**. When the status changes to **Ready to use**, the connection is available for catalog creation.

View an Azure Virtual WAN spoke connection

1. From **Quick Deploy > Microsoft Azure**, expand **Network connections** on the right and select the Virtual WAN spoke connection you want to view. Details include:
   - The number of catalogs, machines, images, and bastions using this connection.
   - The region, Citrix-managed subscription, and customer Virtual WAN hub details.
   - The allocated IP address range and number of available addresses.
   - DNS server configuration.
   - Custom routes configured for the connection.

Manage IPv4 address ranges for an Azure Virtual WAN spoke connection

After creating an Azure Virtual WAN spoke connection, you can expand the allocated network space by adding more IPv4 address ranges to the Citrix-managed spoke virtual network. This capability is

© 1997–2026 Citrix Systems, Inc. All rights reserved.

useful when your existing address range is running low on available IP addresses or when you need to support additional Flex workloads.

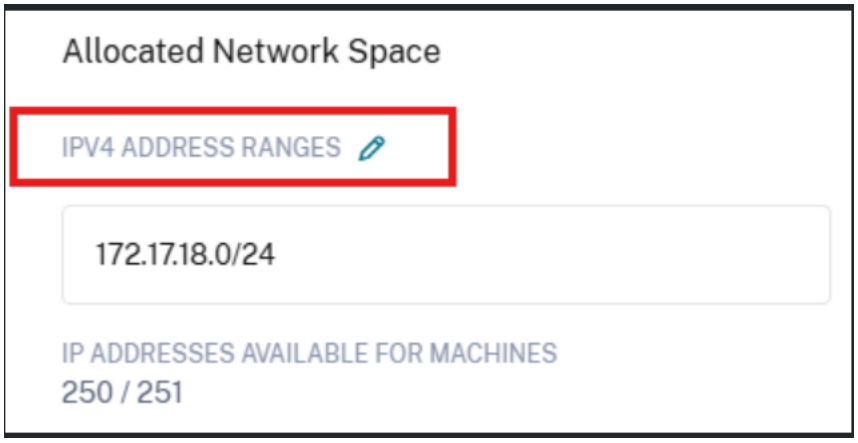
Before adding, modifying, or deleting IPv4 address ranges, ensure the following conditions are met:

- Each address range must be unique within the address space and must not overlap other subnet address ranges in the virtual network.
- Each address range must use Classless Inter-Domain Routing (CIDR) notation. For example, `172.18.0.0/21`.

> **Notes:**
>
> - After adding new IPv4 address ranges, ensure that the corresponding subnets are permitted on your firewalls, routers, and advertised routes. Otherwise, Flex resources using the new ranges will not have end-to-end network connectivity.
> - Before editing an address range, ensure that no existing Flex resources, such as machines or catalogs, are using that subnet. A connection must retain at least one IPv4 address range at all times.
> - Citrix recommends adding new IPv4 address space only when the existing ones are close to exhaustion. This reduces the chances of IP addresses being allocated from different IP address spaces.
> - For Edit and Delete operations, the IPv4 address space must be free (no VDAs, Connectors, Bastions, or Image builders) before the operation is allowed.
> - Azure performs DHCP allocation randomly. The IP address for Flex resources can come from any of the configured IP ranges.

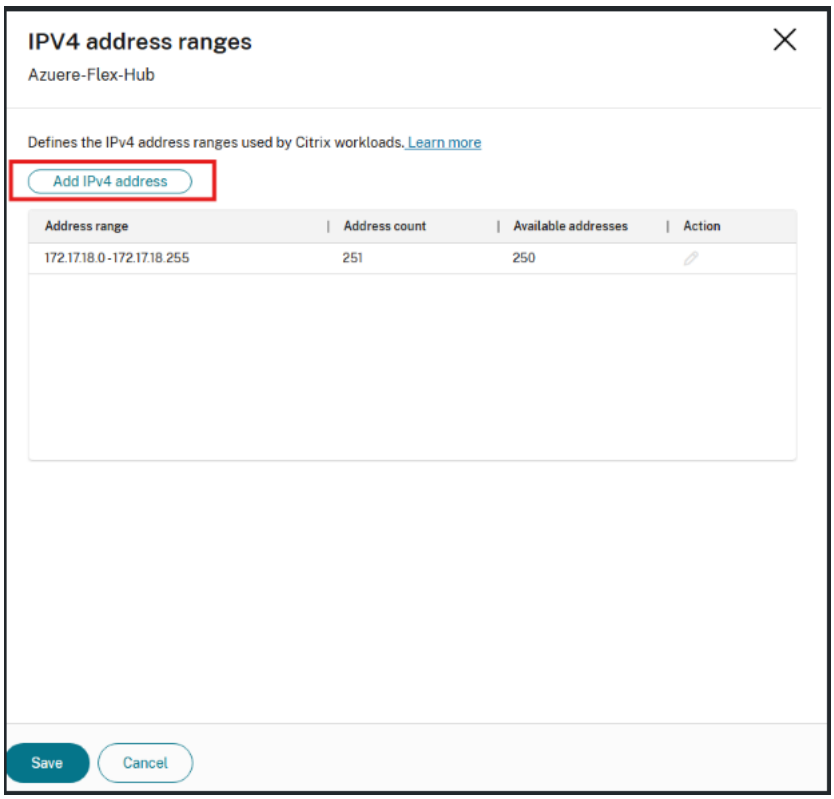
Add an IPv4 address range

1. In Citrix DaaS, go to **Quick Deploy > Microsoft Azure > Network Connections > Virtual WAN Spoke** and select your Azure Virtual WAN spoke connection.
2. In the **Allocated Network Space** section, click the edit icon next to **IPv4 Address Ranges**.



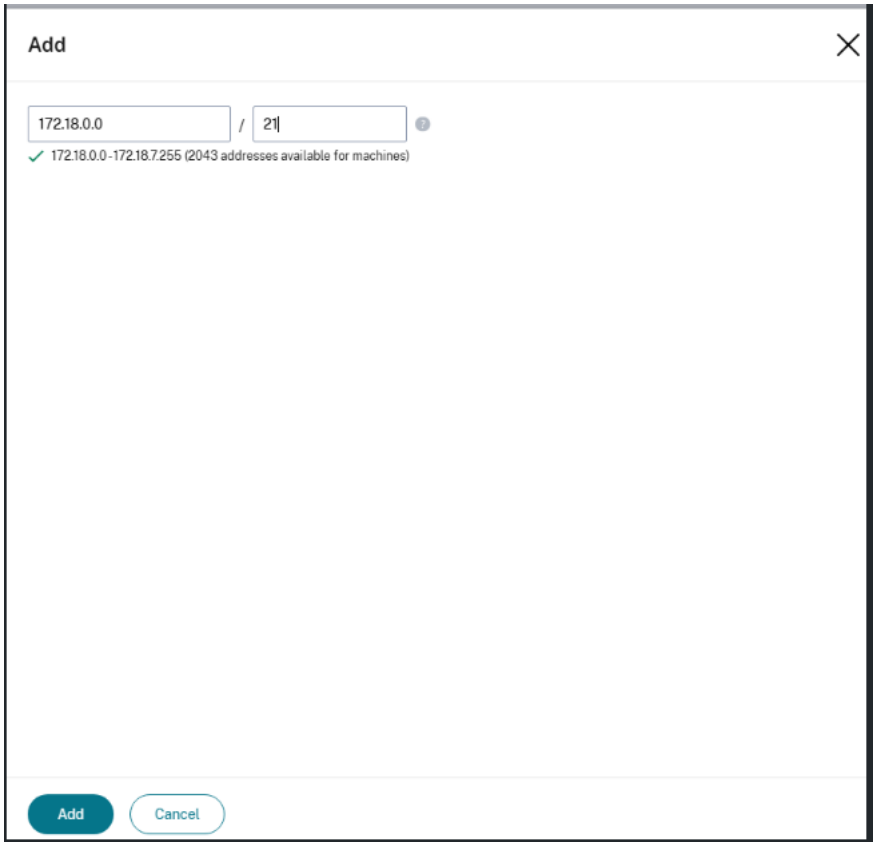
© 1997–2026 Citrix Systems, Inc. All rights reserved.

3. In the **IPv4 address ranges** panel, click **Add IPv4 address**.



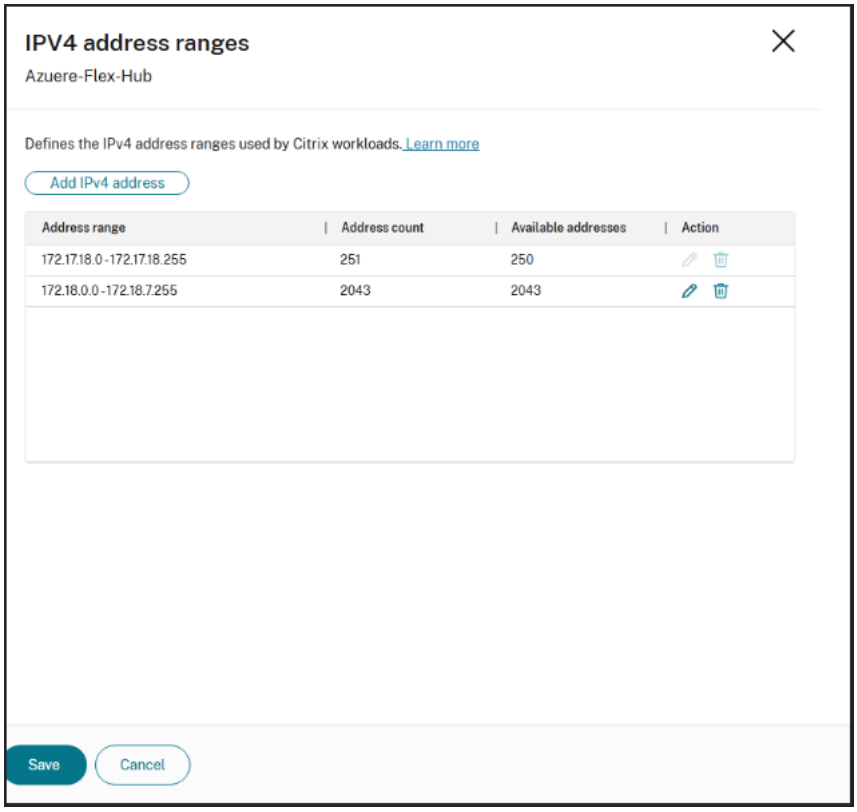
4. In the dialog, enter the IP address and prefix length in CIDR notation. As you type, a preview of the resulting address range and the number of available machine addresses is displayed.

© 1997–2026 Citrix Systems, Inc. All rights reserved.



5. Click **Add**.
6. Review the updated list of address ranges and then click **Save**.

© 1997–2026 Citrix Systems, Inc. All rights reserved.



The new address range is immediately available for use by Flex workloads in the connection.

Edit an IPv4 address range

1. In Citrix DaaS, go to **Quick Deploy > Microsoft Azure > Network Connections > Virtual WAN Spoke** and select your Azure Virtual WAN spoke connection.
2. In the **Allocated Network Space** section, click the edit icon next to **IPv4 Address Ranges**.
3. In the **IPv4 address ranges** panel, click the edit icon in the **Action** column for the range you want to modify.
4. Update the IP address or prefix length as needed. The preview confirms the resulting range and available addresses.
5. Click **Save** to apply the change.

Delete an IPv4 address range Before deleting an address range, ensure that no existing Flex resources, such as machines or catalogs, are using that subnet. A connection must retain at least one IPv4 address range at all times.

1. In Citrix DaaS, go to **Quick Deploy > Microsoft Azure > Network Connections > Virtual WAN Spoke** and select your Azure Virtual WAN spoke connection.
2. In the **Allocated Network Space** section, click the edit icon next to **IPv4 Address Ranges**.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

3. In the **IPv4 address ranges** panel, locate the address range you want to remove and click the delete icon in the **Action** column.
4. Click **Save** to apply the change.

> **Note:**
>
> Before deleting an address range, ensure that no existing Flex resources, such as machines or catalogs, are using that subnet. A connection must retain at least one IPv4 address range at all times.

Delete an Azure Virtual WAN spoke connection

> **Note:**
>
> - Removing a Virtual WAN spoke connection deletes the Citrix managed network spoke from your Virtual Hub. Any catalogs that depend on this connection lose network connectivity to your corporate resources. Delete all associated catalogs before removing the connection. You cannot delete a network connection if it is attached to a catalog.
> - Removing the Flex hub connection does not delete your other Azure Virtual Hub or Virtual WAN. It only removes the Citrix managed network spoke. Your existing VNet connections to the hub are not affected.

1. From **Quick Deploy > Microsoft Azure**, expand **Network connections** on the right.
2. Locate and select the Virtual WAN spoke connection you want to remove.
3. Click **Delete Connection** at the bottom of the page. If this option is unavailable, delete the attached catalog first.
4. Select your authentication method.
5. Select **I understand that deleting a network connection cannot be undone**, then click **Delete**.

   The connection status changes to **Deleting**. When the connection is removed from the list, the Citrix managed network spoke has been detached from your Virtual Hub.

Troubleshooting

Problem: Software fails to download during catalog machine setup.

Symptom: Machines get stuck during provisioning. Logs show a script or download failing.

Cause: Citrix machines cannot reach the internet to download required setup files.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Resolution: Ensure the Custom routes field during connection setup includes a route with destination prefix 0.0.0.0/0 and next hop type Internet. If this was omitted, delete the connection and re-create it with the route included.

Problem: The connection shows `VWanConnectionFailed` status.

Symptom: After completing the wizard, the connection status shows `VWanConnectionFailed`.

Cause: Azure rejected the request to attach the Citrix managed network to the hub. Common causes: The address range overlaps with another network already connected to the hub, or the credentials provided do not have sufficient permissions.

Resolution: Check the ErrorMessage field in the connection status for the specific error text. For address overlap, choose a different non-overlapping CIDR block and re-create the connection. For permissions, ensure the Azure account or service principal has at minimum the Network Contributor role on the Virtual Hub resource group.

Problem: The connection shows `RouteTableFailed` or `NatGatewayFailed` status.

Symptom: The connection status is neither **Ready to use** nor **VWanConnectionFailed**.

Important: In both cases, the hub spoke connection itself succeeded. You can still proceed with catalog creation. The route table or NAT gateway configuration can be retried independently without re-creating the connection. A NAT gateway is automatically created when you create a catalog for this connection.

Resolution: If the issue persists, contact Citrix Support and provide the Citrix-TransactionId so the team can locate the relevant service logs.

Problem: The connection is stuck on Provisioning for more than 10 minutes.

Symptom: The connection status has not changed from Provisioning after 10 or more minutes.

Cause: A background provisioning job might have crashed or timed out.

Resolution: Note the `Citrix-TransactionId` and contact the support team. Once investigated, the request can be resubmitted.

DNS servers

If using virtual network peering, virtual wan peering or a VPN Gateway, one or more valid DNS server entries that can resolve public and private domain names must be added for you to create connections or catalogs.

- DNS entries are validated when you create your connection. If the DNS entry cannot resolve public and private domain names, the create operation fails.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

> **Note:**
>
> The default (Azure-provided) DNS server cannot be used with a virtual network peering or Azure VPN Gateway connection.

  - If you already have DNS server entries under Custom, verify that the entries 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.

- Click **Network Connections** to edit DNS server entries, select the connection you would like to edit, and then select **Edit DNS servers**.

  - If you change any DNS server entries, the VMs continue to use the old DNS server entries until the VM is rebooted.

> **Note:**
>
> Changing DNS server addresses can potentially cause connectivity issues for machines in catalogs that use that connection.

Service endpoints

Azure Storage Service endpoints allow Citrix DaaS Flex VDAs to securely access Azure Storage accounts that are restricted to trusted virtual networks. This is commonly used for Citrix Profile Management stores and FSLogix profile containers hosted in Azure Storage.

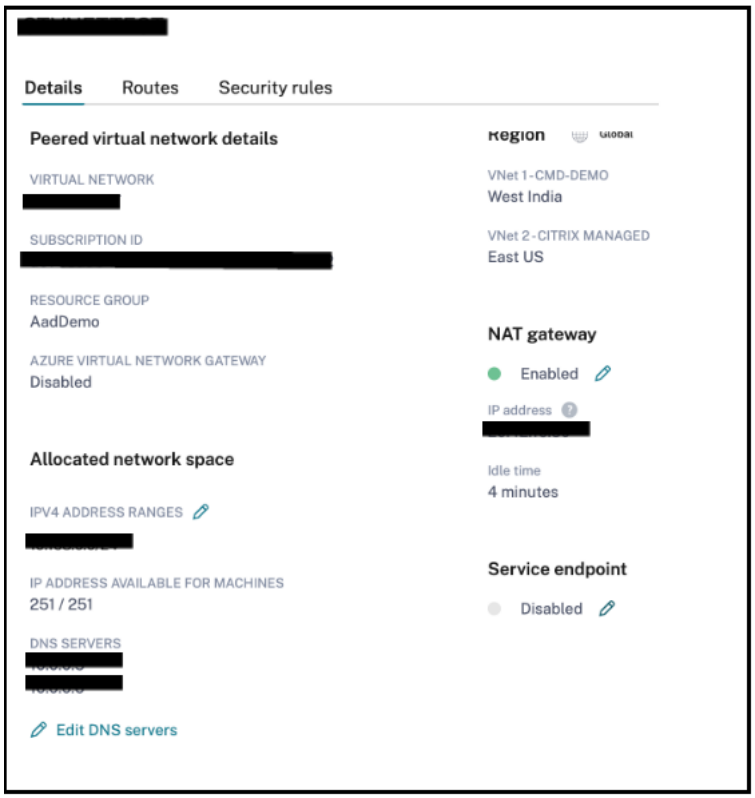
When a Service Endpoint is enabled on a Flex network connection, traffic between Flex VDAs and Azure Storage is routed through the Azure backbone network rather than the public internet to ensure security and compliance.

Enable a Service Endpoint

Open the network connection

1. In DaaS Flex Quick Deploy, navigate to **Network Connections**.
2. Select the Flex network connection.
3. Open the **Details** tab.
4. Locate the **Service endpoint** setting.

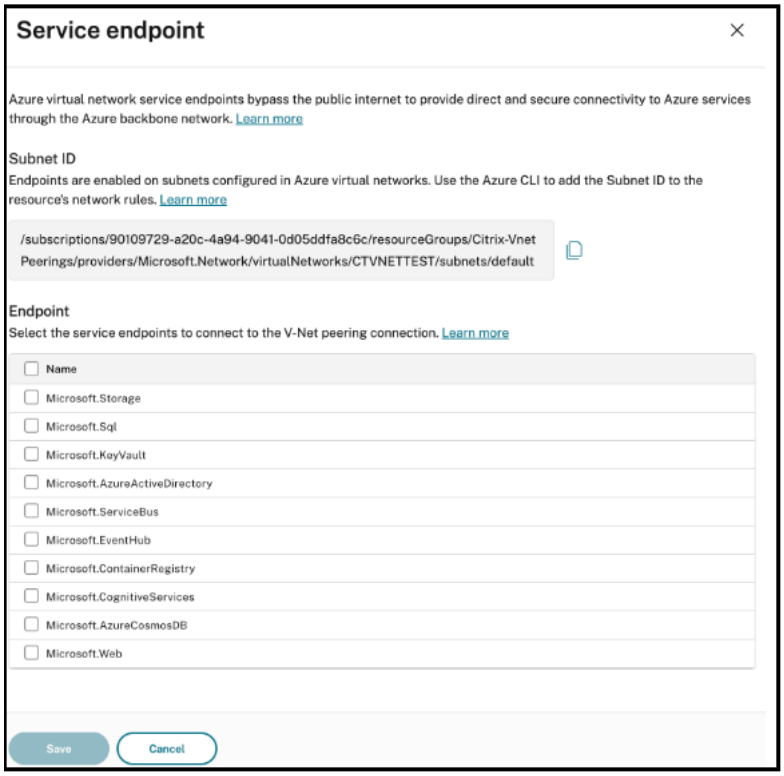
© 1997–2026 Citrix Systems, Inc. All rights reserved.



Review the subnet ID and available endpoints

1. Select the edit (pencil) icon next to **Service endpoint**.
2. Review the service endpoint configuration panel.
3. Copy the displayed subnet ID.
4. Review the list of supported Azure service endpoints.

© 1997–2026 Citrix Systems, Inc. All rights reserved.



5. Select the relevant service endpoint, for example, **Microsoft.Storage**.

Configure Azure Storage network rules

After enabling the Service Endpoint in DaaS Flex Quick Deploy, add the copied Flex subnet ID to the Azure Storage account network rules. This allows Azure Storage to accept connections originating from the Flex subnet through the Service Endpoint.

For more information, see az network VNet subnet update.

Supported network connection types

Service Endpoints are supported on the following Flex network connection types:

- Virtual network peering
- Azure Virtual WAN spoke

Network port management for Citrix-managed VNet connections

Citrix DaaS Flex for Azure now lets administrators configure custom inbound and outbound network port rules for Citrix-managed Azure virtual network connections. This enables you to open specific

© 1997–2026 Citrix Systems, Inc. All rights reserved.

TCP or UDP ports required by applications running on your VDAs without requiring Citrix Support intervention, while maintaining the baseline security posture of the Citrix-managed subscription.

This feature is available for both **Virtual network peering** and **Azure Virtual WAN spoke** connections.

Security model

The Citrix-managed Azure subscription applies a deny-by-default security model using Azure Network Security Groups (NSGs). All traffic not explicitly permitted by a Citrix system rule or a customer-defined custom rule is blocked. Custom rules you add operate alongside Citrix system rules. System rules cannot be modified or deleted.

Default port behavior

The following ports are managed by Citrix system rules and cannot be modified through the self-service port management feature. Attempting to create a Deny rule for ports that are required for HDX™ connectivity is blocked by the system.

Ports reserved by Citrix These ports are always managed by system rules:

Port(s)	Protocol	Purpose
443	TCP	HTTPS —Citrix Cloud™ and Gateway connectivity
80	TCP	HTTP
1494	TCP	ICA® —HDX session traffic
2598	TCP	CGP —session reliability
53	TCP/UDP	DNS
88	TCP/UDP	Kerberos
123	UDP	NTP —time synchronization
135–139	TCP/UDP	RPC / NetBIOS
389	TCP	LDAP
464	TCP/UDP	Kerberos password change
636	TCP	LDAPS
3268–3269	TCP	Global Catalog

© 1997–2026 Citrix Systems, Inc. All rights reserved.

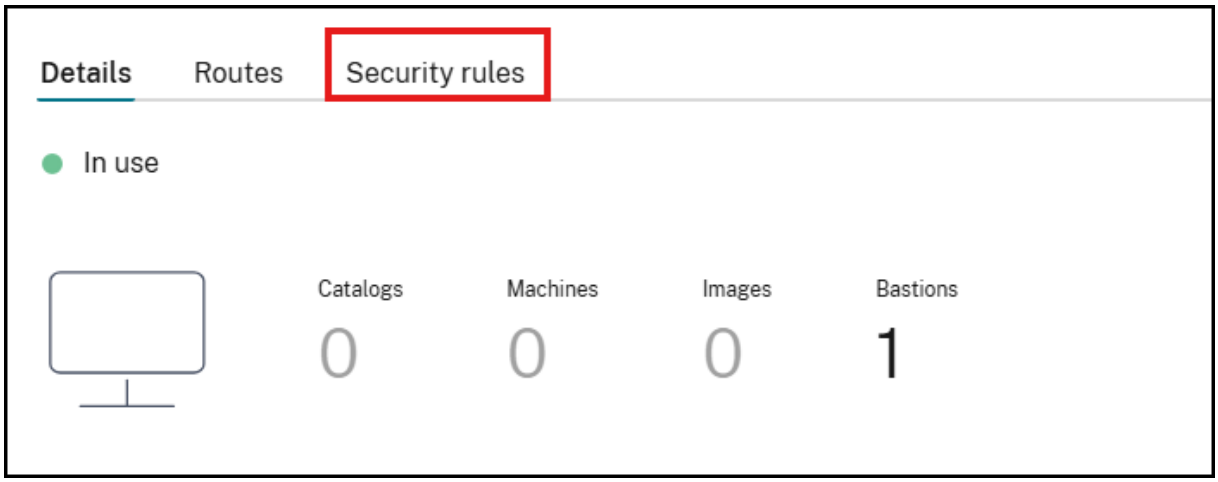
Ports permanently blocked The following ports are blocked by default as a security baseline and cannot be opened through the
self-service port management UI. If your workload requires any of these ports, contact Citrix Support to discuss your use case.

Port(s)	Protocol	Reason blocked
22	TCP	SSH —high risk; use bastion or JIT access instead
23	TCP	Telnet —unencrypted, legacy protocol
20–21	TCP	FTP —unencrypted file transfer
3389	TCP	RDP —direct exposure is a major attack vector
49152–65535	TCP/UDP	Ephemeral range —contact Support for dynamic RPC/VoIP needs

> **Note:**
>
> If your Flex workload requires a permanently blocked port, contact Citrix Support.

Custom port rules

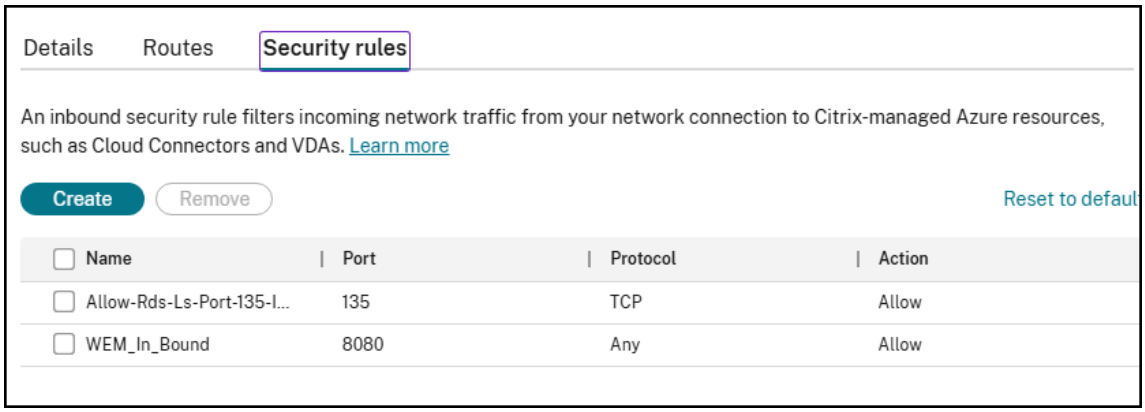
You can create custom rules to allow or deny specific TCP or UDP traffic for your VDA workloads. Custom rules are applied after Citrix system rules and are evaluated by priority order.



Add a custom port rule To add a custom port rule:

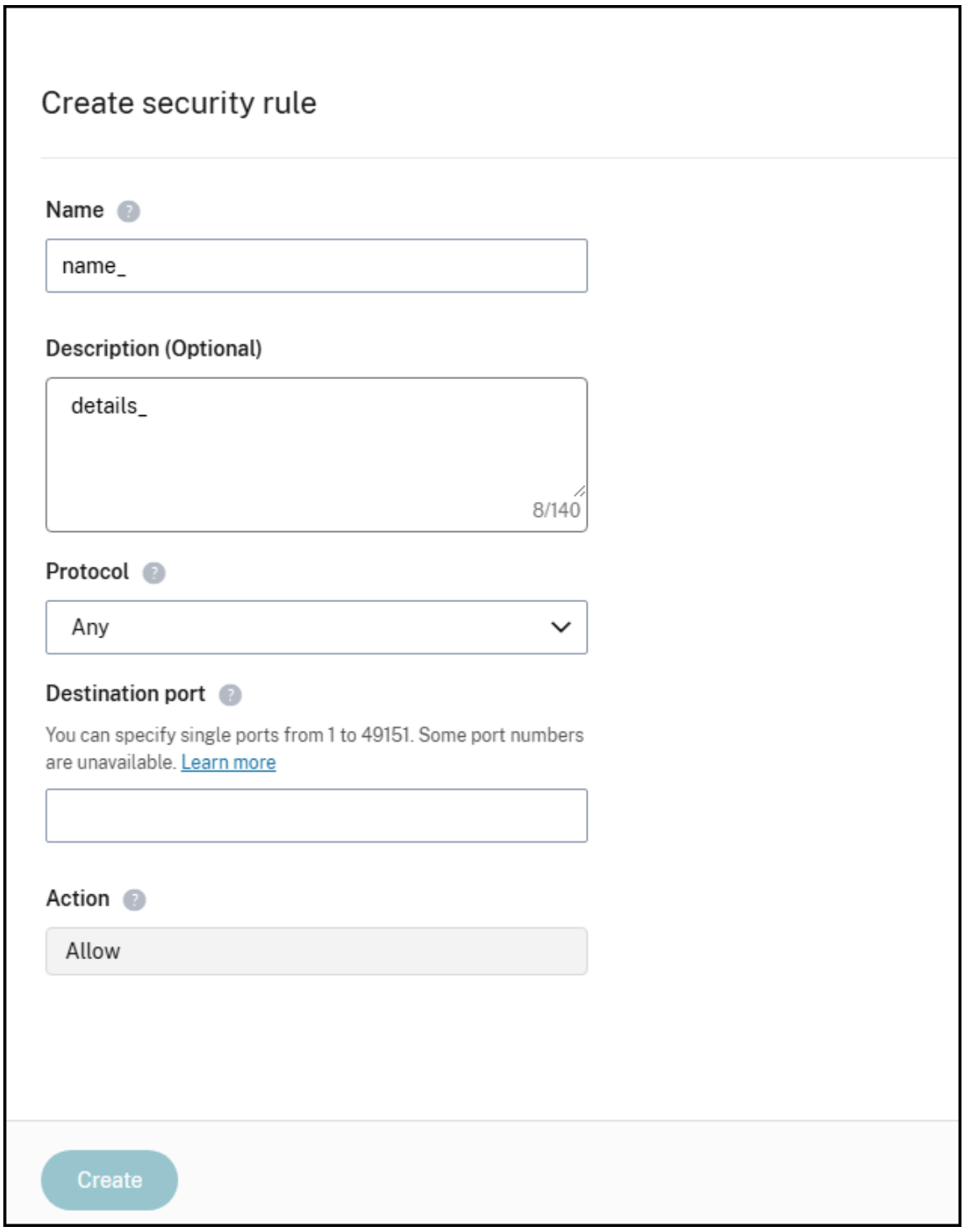
© 1997–2026 Citrix Systems, Inc. All rights reserved.

1. In **Web Studio**, go to **Quick Deploy** > **Microsoft Azure** > **Network connections**.
2. Select the network connection you want to configure.
3. Go to the **Security rules** tab and click **Create**.



4. In the **Create** dialog, configure the fields described in the following table.

© 1997–2026 Citrix Systems, Inc. All rights reserved.



5. Click **Create**. The rule is validated and queued for deployment.
6. Wait for the rule status to change to **Active**. Rule propagation to Azure NSGs takes up to 5 minutes.

The following table describes the fields in the **Create** dialog:

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Field	Description
Name	A descriptive, unique name for the rule (for example, securityrule1).
Port	Destination port or port range (for example, 1433, or 8080–8090).
Protocol	TCP, UDP, or Any.
Action	Allow or Deny.

> **Important:**
>
> If the Azure API call fails during rule propagation, the UI displays a **Failed / Retrying** status. The system retries automatically. Do not delete and re-create the rule during this state.

Guardrails and validation The following validations are enforced when you add a custom rule:

- **Blocking critical ports is prevented**: You cannot create a **Deny** rule for ports 443, 1494, or 2598 toward Citrix Gateway or Citrix Cloud. Doing so disconnects user sessions.
- **Permanently blocked ports**: Rules that target permanently blocked ports (see the preceding table) are rejected at submission time.

Remove a custom rule To remove a custom rule:

1. In the **Security rules** tab, select the rule you want to remove.
2. Click **Remove**.
3. Confirm the removal in the dialog.
4. The rule is removed and the change propagates to Azure NSGs within 5 minutes.

Revert to default configuration If a misconfigured custom rule disrupts VDA connectivity, use the **Revert to Default** function to remove all custom rules and restore the original Citrix-safe configuration immediately.

1. In the **Security rules** tab, click **Revert to Default**.
2. Acknowledge the warning that all custom rules are permanently deleted.
3. Click **Confirm**. Custom rules are removed and Citrix system rules are restored.

> **Important:**

© 1997–2026 Citrix Systems, Inc. All rights reserved.

> **Revert to Default** removes all custom rules. This action cannot be undone. Export or document your custom rules before using this option if you might need to reapply them.

Audit trail Every port rule change is recorded in the Citrix configuration logging system. The audit log
captures the following information for each change:

- Timestamp of the change
- Administrator account that made the change
- Rule details (name, port, action)
- Result (success or failure)

To review port rule changes, access the Configuration Logging node in Web Studio. Filter by the network connection name or by the administrator account to locate specific events.

Port rule reference Use the following guidance when deciding which ports to open for common application scenarios:

Application / use case	Port(s)	Recommended source restriction
SQL Server database access	1433 TCP	App server subnet CIDR only — never Any
WEM agent to connector (if not on 8080)	8080 TCP	Internal subnet only
Web application (HTTP/S)	8080–8090 TCP	Specific IP range or subnet
VoIP / SIP signaling	5060–5061 TCP/UDP	VoIP provider IP range
Custom LDAP (non-standard port)	Custom TCP	Domain controller subnet only
Outbound to on-premises data center	As required	Specific on-premises CIDR through VNet peering

Limitations

- Port rules apply to all machines in all catalogs using the network connection. Per-catalog or per-machine rules are not supported.
- Permanently blocked ports (22, 23, 20/21, 3389, and ports above 49151) cannot be opened through the self-service UI. Contact Citrix Support for exceptions.
- Rule propagation can take up to 5 minutes. Do not assume that a rule is active immediately after saving.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Effective routes visibility for network connections

Citrix DaaS Flex provides visibility into the effective Azure routes applied to a network connection. For a given on-premises connection, the system resolves the corresponding Azure context —subscription, resource group, and virtual network —and retrieves the effective route table from a network interface in that virtual network. Administrators can use this view to verify routing configuration and diagnose connectivity issues without leaving the Citrix management console.

The effective route table reflects what Azure is actually applying, including system routes, BGP-learned routes, and user-defined routes (UDRs). This differs from the configured route table, which does not account for BGP advertisements or system-level overrides.

View effective routes

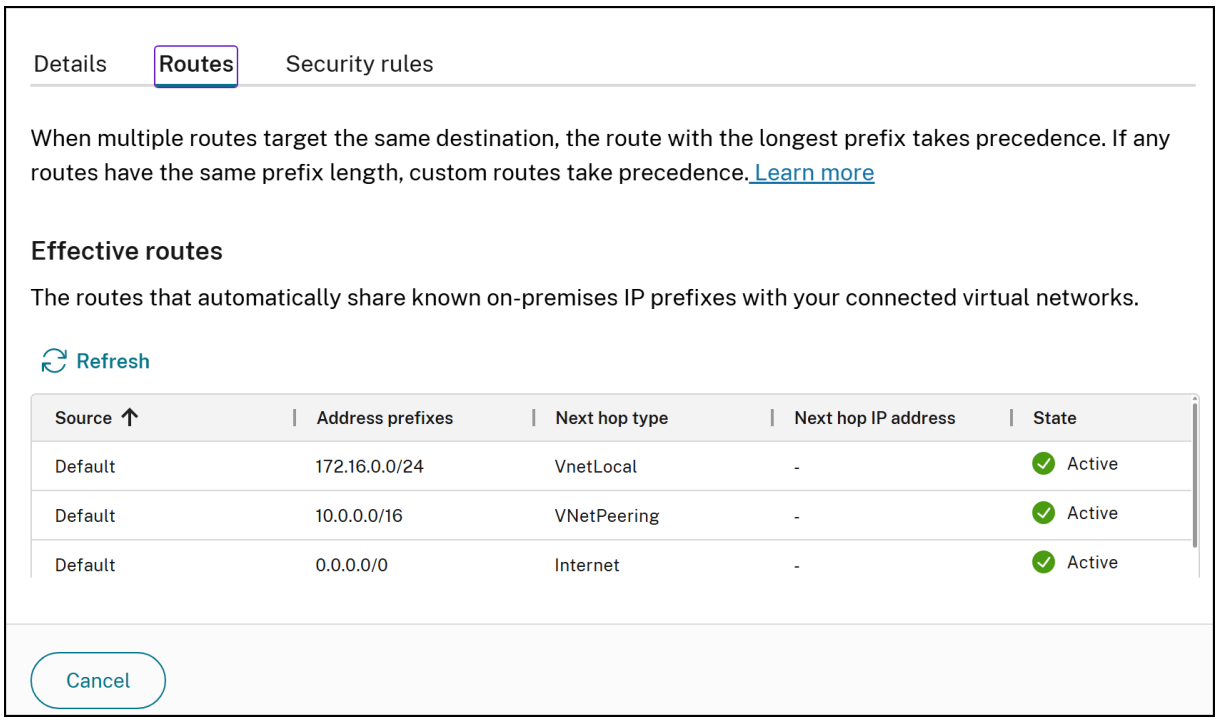
1. In the Quick Deploy UI, navigate to **Network Connections**.
2. Select the on-premises connection for which you want to view routing information.
3. Select the **Routes** tab.

   When multiple routes target the same destination, the route with the longest prefix takes precedence. If any routes have the same prefix length, custom routes take precedence.
4. Under **Effective routes**, review the routes that automatically share known on-premises IP prefixes with your connected virtual networks. Select **Refresh** to retrieve the latest route table from Azure.

The effective route table displays the following information for each route:

Column	Description
Source	The origin of the route, such as **Default** for system routes.
Address prefixes	The destination address range in CIDR notation, for example, `172.16.0.0/24`.
Next hop type	Where traffic for the prefix is routed, such as **VnetLocal**, **VNetPeering**, or **Internet**.
Next hop IP address	The IP address of the next hop, when applicable.
State	The current status of the route, such as **Active**.

© 1997–2026 Citrix Systems, Inc. All rights reserved.



Resource locations

May 11, 2026

Citrix automatically creates a resource location and Cloud Connectors when you create the first catalog for publishing desktops and apps.

In the subscriptions pane, if you select a subscription:

- The **Details** tab shows the number and names of catalogs and images in the subscription. It also indicates the number of machines that can deliver desktops or apps. That count does not include machines used for other purposes, such as images, Cloud Connectors, or RDS license servers.
- The **Resource Locations** tab lists each resource location. Each resource location entry includes the status and address of each Cloud Connector in the resource location.

The ellipsis menu in a resource location's entry contains the following actions:

- **Run Health Check**: Selecting **Run Health Check** starts the connectivity check immediately. If the check fails, the Cloud Connector's state is unknown, because it is not communicating with Citrix Cloud.
- **Restart Connectors**: Citrix recommends restarting only one Cloud Connector at a time. Restarting takes the Cloud Connector offline.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

    - Select the check box for the Cloud Connector you want to restart. Click **Restart**.

- **Add Connectors**: Adding a Cloud Connector typically takes 20 minutes to complete. Provide the following information:

    - How many Cloud Connectors to add
    - Domain service account credentials, which are used to join the Cloud Connector machines to the domain
    - Machine performance
    - Azure resource group. The default is the resource group last used by the resource location.
    - Organizational Unit (OU). The default is the OU last used by the resource location.
    - Whether your network requires a proxy server for internet connectivity. If you indicate **Yes**, provide the proxy server FQDN or IP address, and port number.
    - When you're done, click **Add Connectors**.

- **Delete Connectors**: If a Cloud Connector cannot communicate with Citrix Cloud, and a restart does not resolve the issue, Citrix Support might recommend deleting that Cloud Connector.

    - Select the check box for the Cloud Connector you want to delete. Then click **Delete** When prompted, confirm the deletion.
    - You can also delete an available Cloud Connector. However, if deleting that Cloud Connector would result in fewer than two available Cloud Connectors in the resource location, you're not allowed to delete the selected Cloud Connector.

- **Select Update Time**: Citrix automatically provides software updates for the Cloud Connectors. During an update, one Cloud Connector is taken offline and updated, while other Cloud Connectors remain in service. When the first update completes, another Cloud Connector is taken offline and updated. This process continues until all Cloud Connectors in the resource location are updated. The best time to start updates is usually outside your typical business hours.

    - Choose the time to begin updates, or indicate that you want updates to start when an update is available. When you're done, click **Save**.

- **Rename**: Enter the new name for the resource location. Click **Save**.
- **Configure Connectivity**: Indicate whether users can access desktops and apps through the Citrix Gateway service, or only from within your corporate network.

Customer-managed encryption keys for VM disks

May 11, 2026

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Customer Managed Encryption Keys (CMEK) for VM disks offers customers control over their data security to manage their encryption keys independently, ensuring compliance with strict security policies and regulations while mitigating risks associated with third-party data breaches. This allows customers to gain full control of their encryption lifecycle, reducing dependency on platform-managed keys. This autonomy ensures their data remains inaccessible to unauthorized parties, even in the event of platform-level vulnerabilities. IT administrators benefit from greater flexibility and security alignment with internal policies.

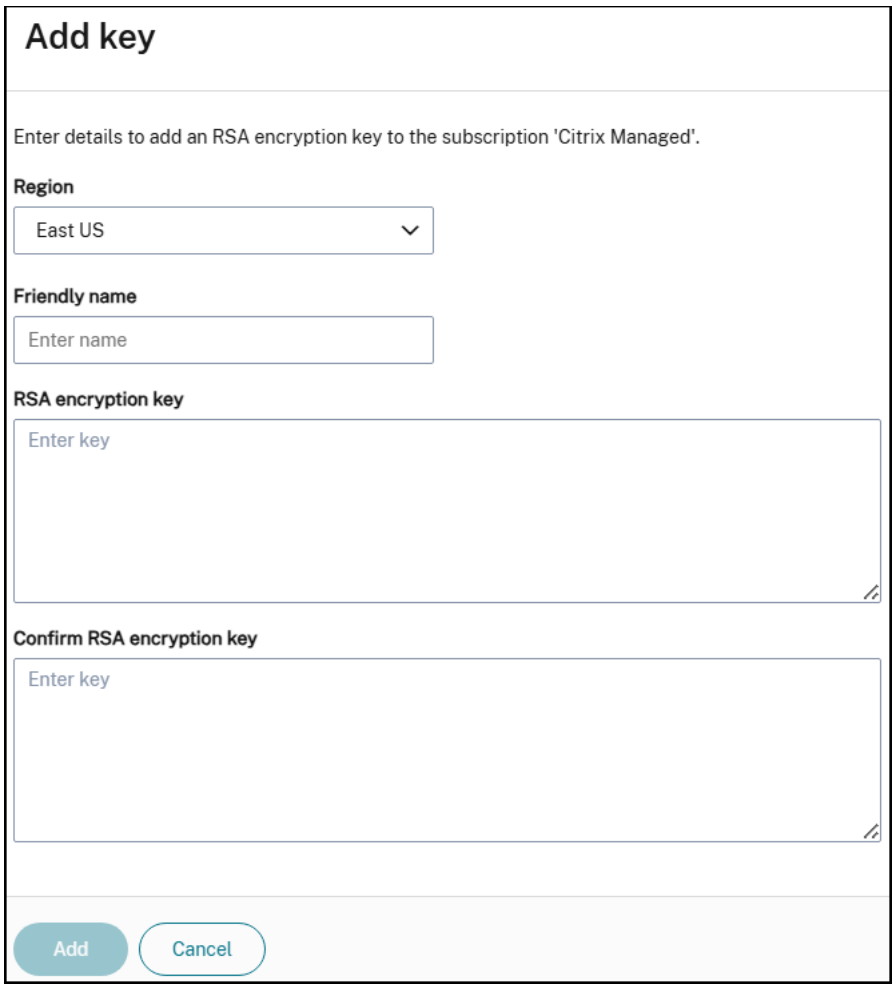
Add an encryption key

1. From the Citrix DaaS Flex dashboard, navigate to **Cloud subscriptions**.
2. Select the relevant resubscription, go to **Customer-managed encryption keys** tab.
3. Click **Add key**.



4. Enter details, and click **Add**.

© 1997–2026 Citrix Systems, Inc. All rights reserved.



Once the key is added, it can be used later when importing images from Azure.

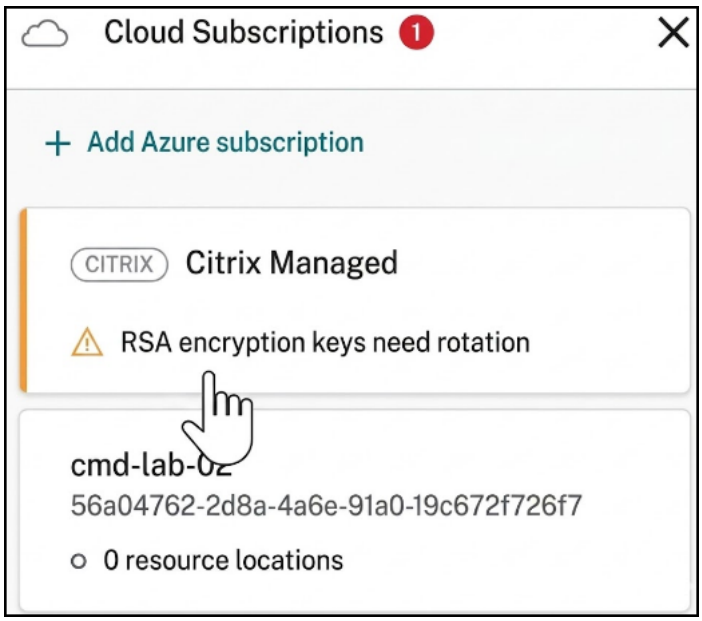
Delete an encryption key

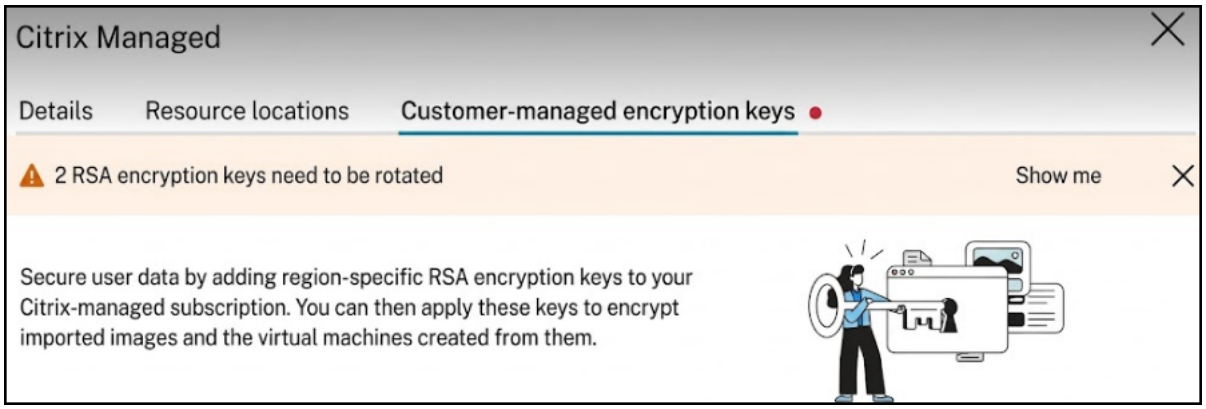
1. From the Citrix DaaS Flex dashboard, navigate to **Cloud subscriptions**.
2. Select the relevant resubscription, go to **Customer-managed encryption keys** tab.
3. Locate the key that needs to be deleted from the existing keys table and then from the ellipsis menu, select **Delete** key.

Rotate an encryption key

If a key's rotation time has expired, the dashboard displays warning message.

© 1997–2026 Citrix Systems, Inc. All rights reserved.





To rotate an encryption key:

1. From the Flex dashboard, navigate to **Cloud Subscriptions > Customer-managed encryption keys** tab.
2. Locate the key that needs rotation from the existing keys table, and then from the ellipsis menu, select **Rotate key**.

Images

September 21, 2026

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

Citrix provides three options for images:

© 1997–2026 Citrix Systems, Inc. All rights reserved.

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

When you create a catalog, Citrix DaaS Flex verifies that the image meets prerequisites for deploying a catalog.

Citrix prepared images

Citrix DaaS Flex provides prepared images that can be deployed to a catalog or used as a starting point to customize your image. The following configurations are offered:

- Windows 11 Pro (single-session)
- Windows Server 2019 (multi-session)
- Windows Server 2022 (multi-session)
- Windows Server 2025 (multi-session)
- Linux Ubuntu 22.04 LTS (single-session)
- Linux Ubuntu 22.04 LTS (multi-session)

The Citrix-prepared images have both a **current version** and a **Long Term Service Release (LTSR) version** of the Citrix Virtual Delivery Agent (VDA) and Citrix Optimizer. Citrix prepared images will be updated with the latest Cumulative Update (CU) and LTSR versions as they become available.

Citrix-prepared images are notated in the user interface as **CITRIX**.

Prepare a new image

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

Requirements:

- Know the performance characteristics that the machines need. For example, running CAD apps might require different CPU, RAM, and storage than other office apps.
- If you plan to use a connection to your on-premises resources, set up that connection before creating the image and the catalog. For details, see Network connections.

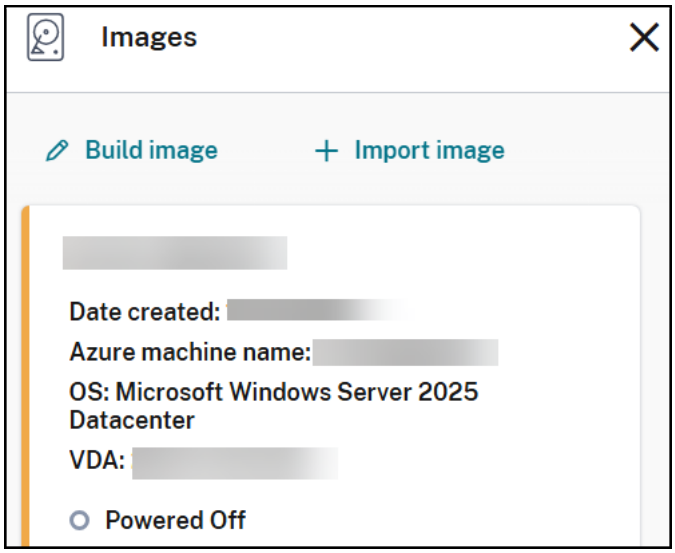
© 1997–2026 Citrix Systems, Inc. All rights reserved.

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

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

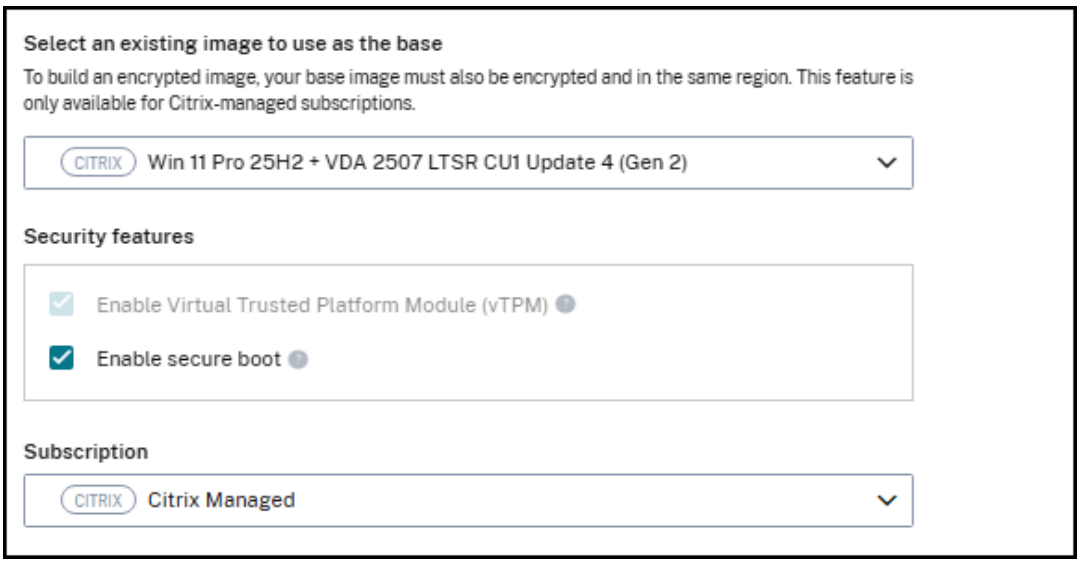
Create an image

1. From the Citrix DaaS Flex dashboard, expand **Images** on the right.
2. Click **Build Image**.



3. On the **Build image** page, enter values in the following fields:
   a) **Name the new image**: Enter a name for the new image.
   b) **Select an existing image to use as the base**: Select an existing image. This is the base image that is used to create the new image. Select a Gen 2 base image from the image list. The VM generation is detected automatically.

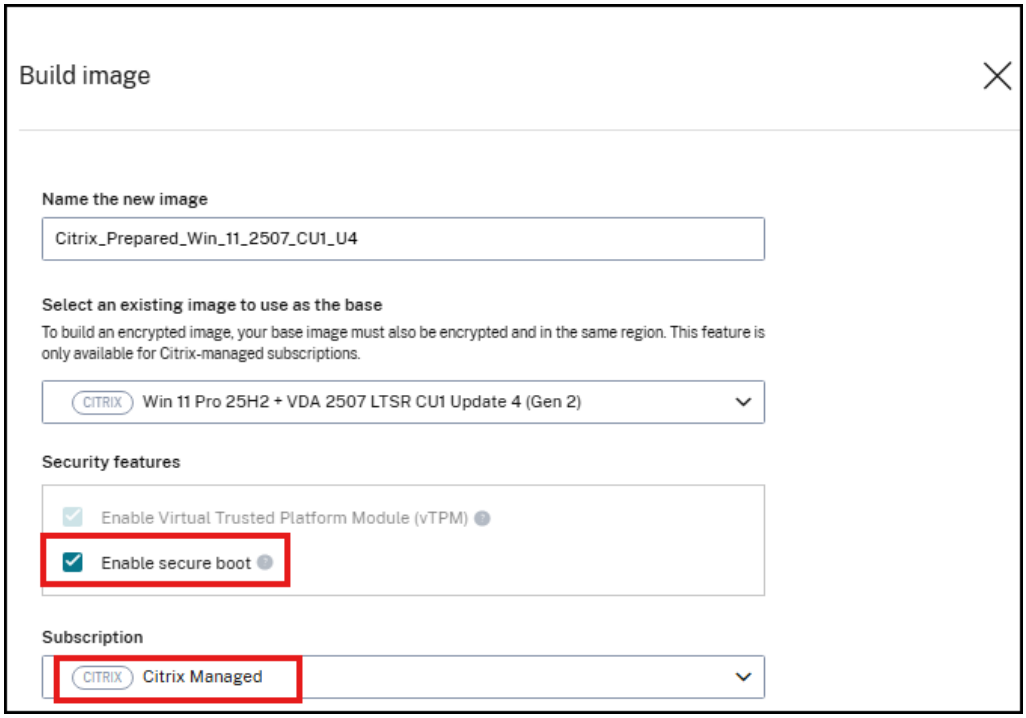
© 1997–2026 Citrix Systems, Inc. All rights reserved.



i. **Security features**: The **Security features** panel appears only when a Gen 2 image is selected.

- **Enable Virtual Trusted Platform Module (vTPM)** is enabled by default and cannot be changed.
- **Enable Secure Boot** is enabled by default. You can enable or disable this option.

If your configuration requires it, enter the Azure-generated URL for the Secure Boot guest disk. If you disable **Enable Secure Boot**, a best-practice deviation warning is displayed. Review and confirm before proceeding.



© 1997–2026 Citrix Systems, Inc. All rights reserved.

> **Note:**
>
> Gen 1 images do not support Trusted Launch. The **Security features** panel does not appear when a Gen 1 image is selected in the **Build image** wizard.

c) **Subscription**: Select an Azure subscription. For details, see Azure subscriptions.

d) **Network connection**: Select No connectivity or a previously created connection.

e) **Region**: (Available only for No connectivity.) Select a region where you want the machine containing the image to be created. If connectivity is configured, the catalog is created in the region of the connectivity configuration.

f) **Domain type**: Select the domain type: Active Directory or non-domain-joined.

- If you select Active Directory, select or add a domain. Specify an OU (optional), service account name, and password.

g) **Set logon credentials for the image building machine**: You will use these credentials later when you connect (RDP) to the machine containing the new image, so that you can install apps and other software.

h) **Size of the image building machine**: Select the CPU, RAM, and storage information for the machine that runs the image. Select a machine performance that meets your apps' requirements.

i) **Restricted IP access**: Citrix requires restricting the Image Builder machine to a smaller range than permitted by the network connection. Select **Add IP addresses** and then enter the desired IP addresses.

j) **Restricted access duration:** Citrix requires restricting Image Builder machine access to a specific time-based duration. You can choose between 2, 4, and 8-hour durations. Once the time expires, any open machine sessions, firewall rules, and network routes will be closed.

k) Optionally add up to 1024 characters of notes. After the image is created, you can update the notes from the image's details display.

l) When you're done, click **Build Image**.

An image can take up to 30 minutes to build. On the Citrix DaaS Flex dashboard, expand **Images** on the right to see the current state.

Configurable OS disk size for image builds

When building a master image in Citrix DaaS Flex for Azure, you can now select the **OS disk size** for the image building machine. This lets you accommodate applications or operating system

© 1997–2026 Citrix Systems, Inc. All rights reserved.

configurations that require more disk space than the default 128 GB allocation. The disk size you select when building the image determines the OS disk size for the VDAs provisioned from that image.

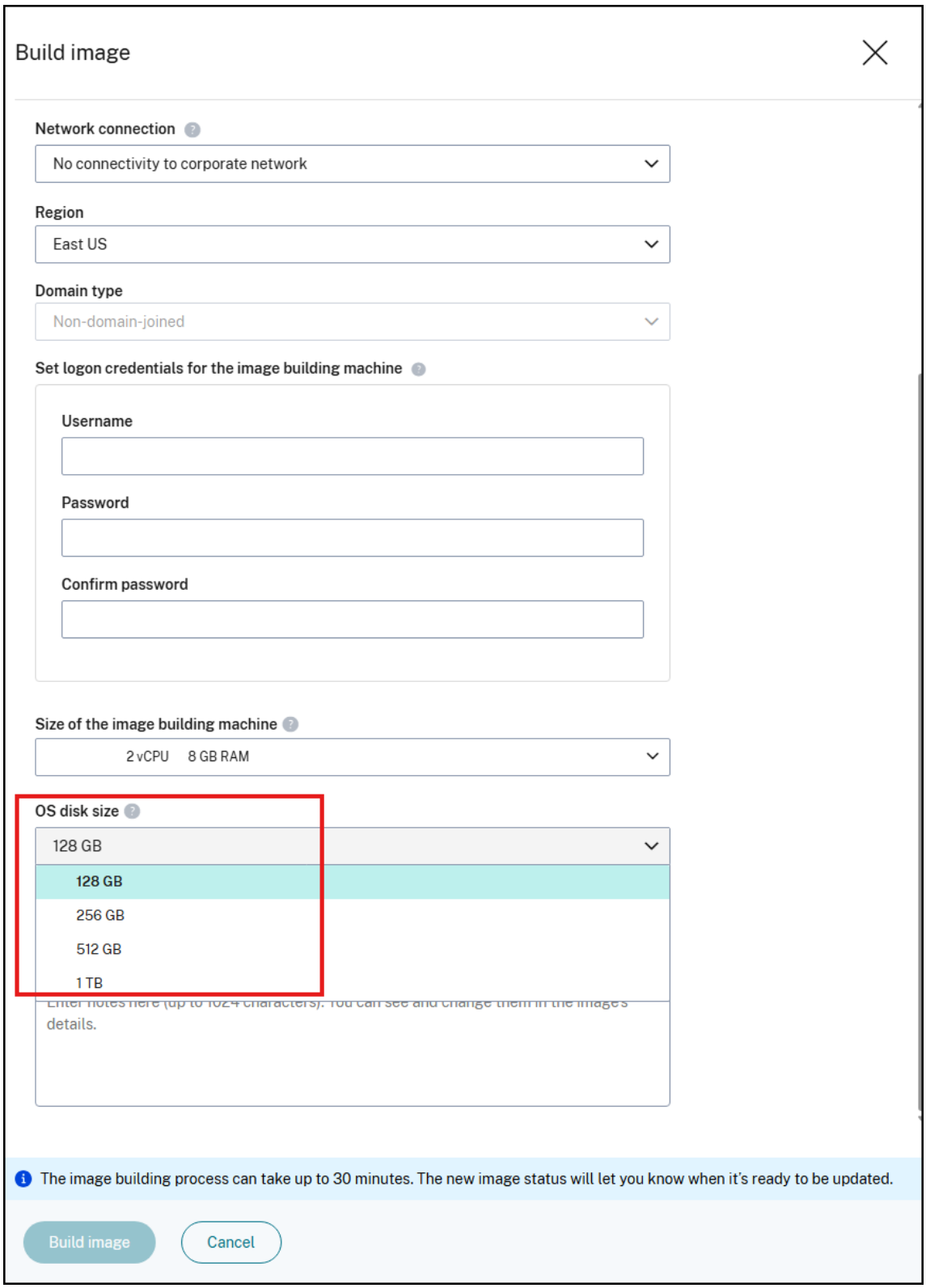
> **Important:**
>
> Selecting a disk size larger than 128 GB can incur additional credit charges. Credit consumption depends on the disk size (128 GB, 256 GB, 512 GB, or 1 TB), the allocation type (persistent or non-persistent), and the storage type (Standard SSD or Premium SSD).

Supported machine types All machine types support configurable OS disk sizes. You can select a larger OS disk size
(256 GB, 512 GB, or 1 TB) for any machine type and session configuration.

Configure OS disk size during image build To select a custom OS disk size when building an image:

1. In **Quick Deploy**, go to **Images** and select **Build image**.
2. Complete the image build form as usual. In the **Size of the image building machine** field, select the machine size appropriate for your workload.
3. In the **OS Disk Size** field (located below the machine size field), select the disk size for the OS disk:
    - **128 GB** (default)
    - **256 GB**
    - **512 GB**
    - **1 TB**

© 1997–2026 Citrix Systems, Inc. All rights reserved.



4. If you select a disk size larger than 128 GB, hover over the tooltip next to **OS disk size** to review the billing advisory: *Depending on your selection, additional credit charges may incur*

© 1997–2026 Citrix Systems, Inc. All rights reserved.

during catalog creation.

5. Complete the remaining image build configuration and click **Build image**.

> **Note:**
>
> The **OS Disk Size** setting applies to the image building machine and determines the OS disk size of all VDAs provisioned from that image. You cannot change the disk size after the image is built. You must build a new image if a different disk size is required.

View disk size in image details After an image is built, the selected disk size appears in the image details pane. In the top
summary card of the image details view (alongside **OS**, **Virtual Delivery Agent**, and **Machine generation**), a **Disk Size** field shows the configured disk size:

- **128 GB**
- **256 GB**
- **512 GB**
- **1 TB**

Disk size and catalog creation When you create a catalog from a master image, Citrix DaaS Flex uses the OS disk size of the image
to determine the disk size for the VDA machines in the catalog. Before creating a catalog from a larger-disk image, review the credit consumption of the larger disk size. Credit consumption depends on the disk size (128 GB, 256 GB, 512 GB, or 1 TB), the allocation type (persistent or non-persistent), and the storage type (Standard SSD or Premium SSD).

Connect to a new image and customize it

After a new image is created, its name is added to the images list, with a status of **Install apps and updates**. To customize that image, download the RDP file. Use the RDP file to connect to the image and customize the software and configurations through that connection.

1. From the Citrix DaaS Flex dashboard, expand **Images** on the right and select the image you want to connect to customize.
2. Click **RDP to Public Address** or **RDP to Private Address** based on your preference and connectivity.
    - The image machine might power off if you do not RDP to it shortly after it's created. This saves costs. If that happens, click **Power On**.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

3. Open the RDP file. Opening the file 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, customize the machine to meet the needs of your use case. Do not Sysprep the image.
5. When you're done customizing the new image, return to **Images** and click **Finish build**. The new image automatically undergoes validation testing.

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

On the Citrix DaaS Flex dashboard, the images display on the right indicates how many catalogs and machines use each image.

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

Import an image from Azure

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

Imported image requirements

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

- **Supported OS**: The image must be a supported OS. To check a Windows OS version, run `Get-WmiObject Win32_OperatingSystem`.
- **Supported generation**: Generation 1 virtual machines support most guest operating systems. Generation 2 virtual machines support most 64-bit versions of Windows and more current version of Linux operating systems.
- **Not generalized**: The image must not be generalized.
- **No configured Delivery Controllers**: Ensure that no Citrix Delivery Controllers are configured in the image. Ensure that the following registry keys are cleared.
  - `HKLM:\SOFTWARE\Citrix\VirtualDesktopAgent\ListOfDDCs`
  - `HKLM:\SOFTWARE\Policies\Citrix\VirtualDesktopAgent\ListOfDDCs`
  - `HKLM:\SOFTWARE\Citrix\VirtualDesktopAgent\FarmGUID`

© 1997–2026 Citrix Systems, Inc. All rights reserved.

    - `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 Citrix VDA version 2507 or higher installed.
    - Windows: To check, use `Get HKLM:\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\Citrix Virtual Desktop Agent`. For installation guidance, see Install VDAs.
    - Red Hat Enterprise Linux and Ubuntu: For installation guidance, see Linux Virtual Delivery Agent.
- **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 Citrix DaaS Flex dashboard, expand **Images** on the right.
2. Click **Import image**.
3. Choose how to import the image.
    - For managed disks, use the export feature to generate a SAS URL. Set the expiration time to 7200 seconds or more.
    - For VHDs in a storage account, choose one of the following:
        - Generate a SAS URL for the VHD file.
        - Update the access level of a block storage container to blob or container. Then, get the file's URL.
4. If you select:
    - **Browse storage account**:
        a) Select a subscription, resource group, storage account, and image.
        b) Name the image.
    - **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.
        c) Name the image.

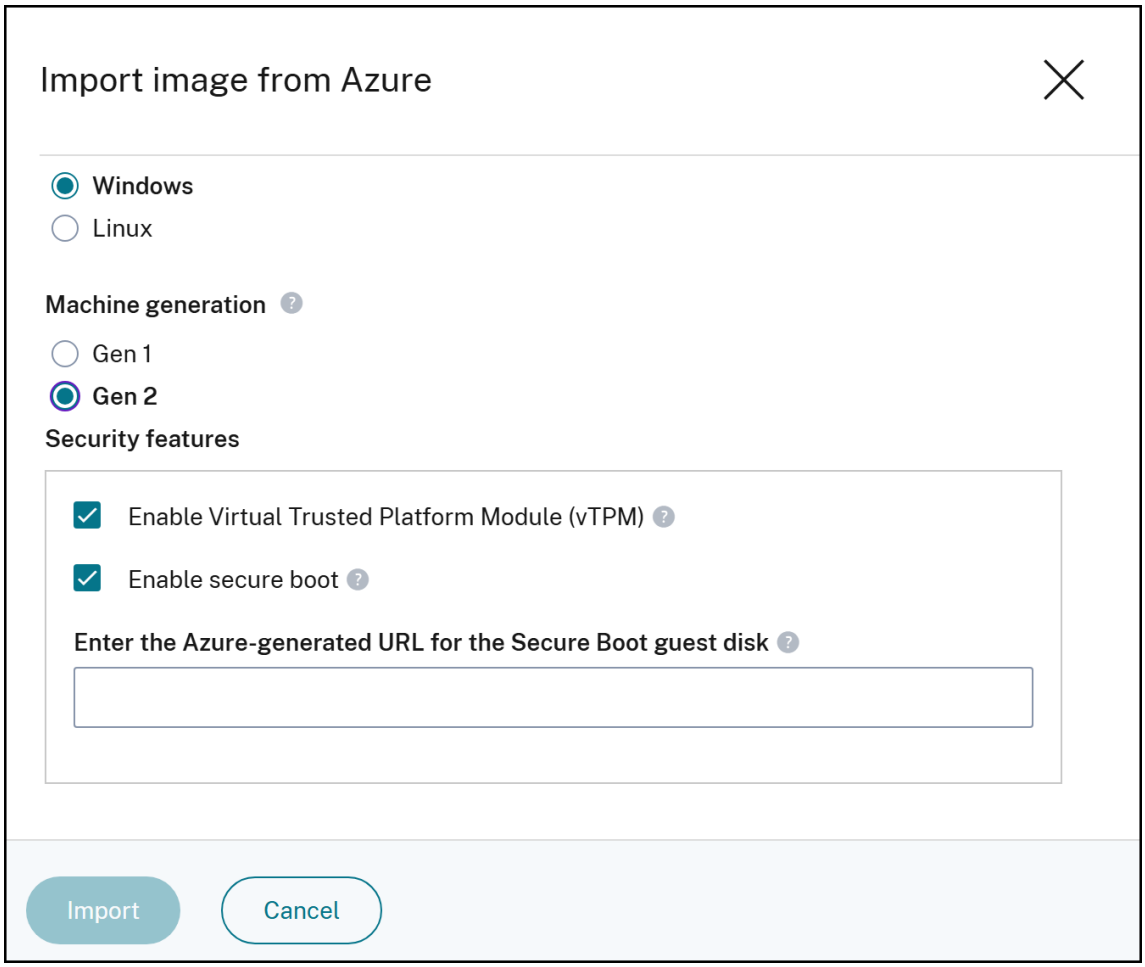
© 1997–2026 Citrix Systems, Inc. All rights reserved.

5. Select the **OS type**: **Windows** or **Linux**.
6. Under **Machine generation**, select **Gen 1** or **Gen 2**.

   For both **Browse storage account** and **Azure public URL**, when the **OS type** is **Windows** and the **Machine generation** is **Gen 2**, the **Security features** panel appears with the following options:

   - **Enable Virtual Trusted Platform Module (vTPM)**
   - **Enable Secure Boot**

   Both options are enabled by default, and you can enable or disable either option. If your configuration requires it, enter the Azure-generated URL for the Secure Boot guest disk.



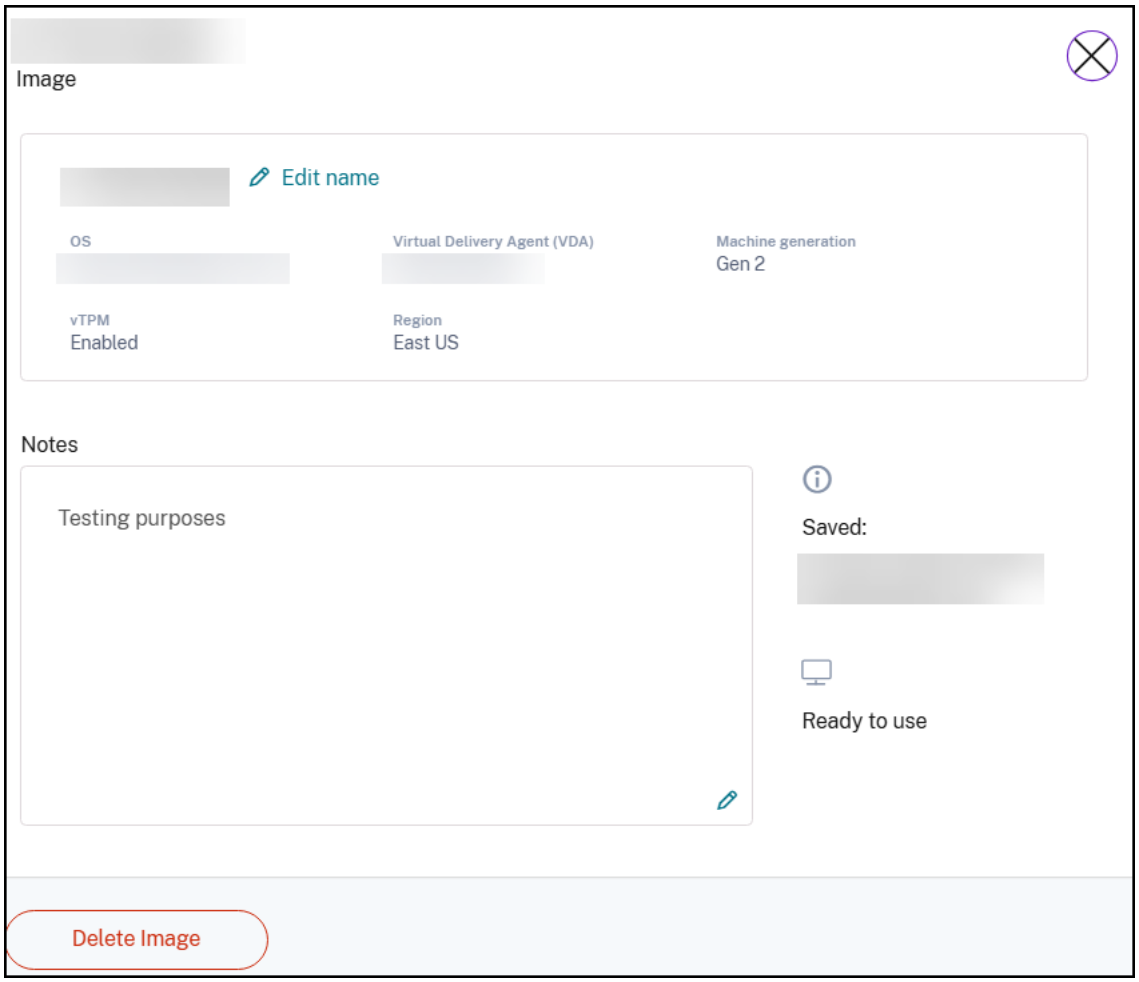
7. When you are done, click **Import**.

Display and manage image information

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

© 1997–2026 Citrix Systems, Inc. All rights reserved.

2. Click an image to display its details.



3. From the details card, you can:

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

Delete an image

1. From the Citrix DaaS Flex dashboard, expand **Images** on the right.
2. Select the image you want to delete.
3. Click **Delete Image** and confirm the deletion.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Create catalogs and add users

September 29, 2026

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

Machine types

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

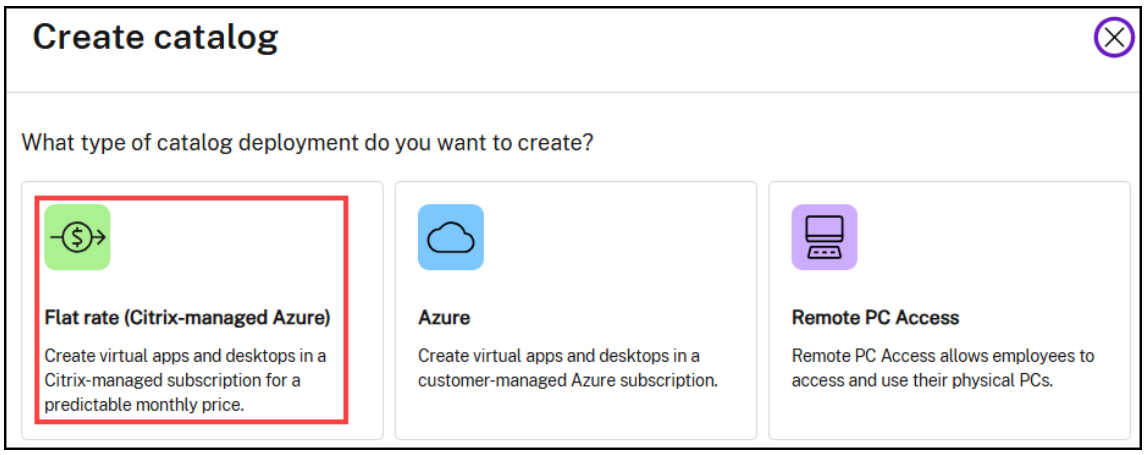
- **Static**: The catalog contains single-session static machines (also known as personal, dedicated, or persistent desktops). Static means that when a user starts a desktop, that desktop "belongs" to that user. Any changes that that user makes to the desktop are retained at logoff. Later, when that user returns to and starts a desktop, it is the same virtual machine.
    - **Associated personas**: Knowledge worker, Power worker, and custom persona.
- **Random**: The catalog contains single-session random machines (also known as non-persistent or pooled 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.
    - **Associated personas**: Knowledge worker, Power worker, and custom persona.
- **Multi-session**: The catalog contains machines that deliver apps, desktops, or both. More than one user can access each of those machines simultaneously. Users can launch a desktop or apps from their workspace.
    - **Associated personas**: Task worker (medium) (8 users per VM), Task worker (heavy) (4 users per VM), and custom persona.

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

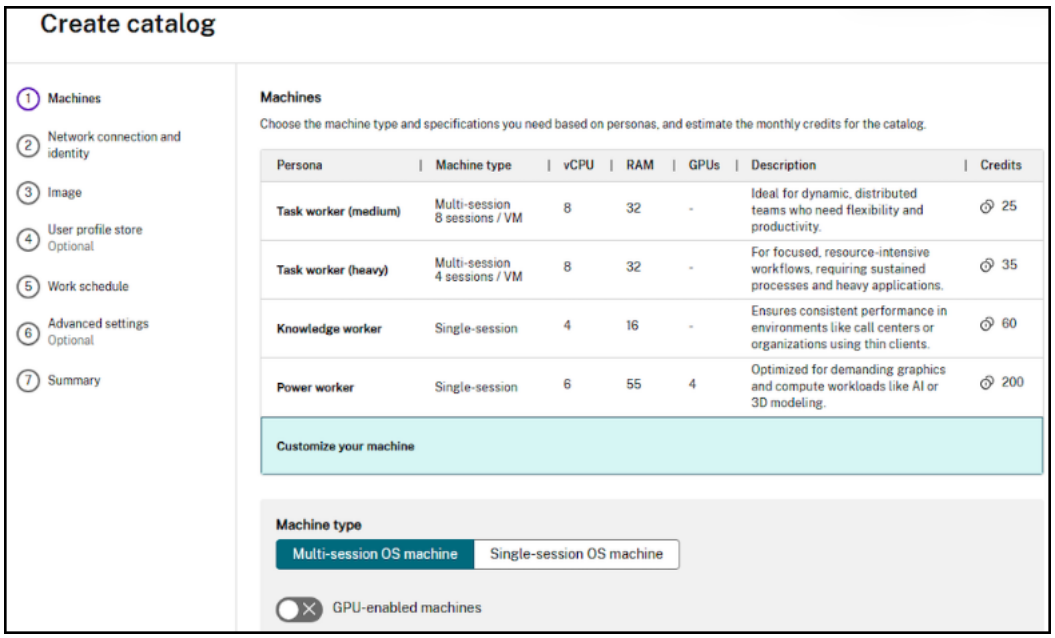
Create a catalog

1. From the Citrix DaaS Flex dashboard, click **Create catalog**.
2. Select **Flat rate (Citrix-managed Azure)**.

© 1997–2026 Citrix Systems, Inc. All rights reserved.



3. Choose the persona of the catalog.



- If selecting a Knowledge worker or Power worker, choose whether the VDAs must be delivered as static or random desktops.
- If selecting a custom persona, choose the specifications based on the requirements of your users.

  > **Note:**
  >
  > Flex credits for custom personas varies based on the specifications.

- Input the **Number of unique users** who will access the catalog.

4. Configure the **Network connection and identity**.

   a) **Subscription**: Select an Azure subscription. For details, see Azure subscriptions.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

b) **Network connection**: Select the connection to use for accessing resources in your network. For details, see Network connections.

c) **Region**: Select a region where you want the desktops created. Consider selecting a region close to your users. If you selected to use a connection, the catalog uses that network connection's region.

d) **Domain configuration**: Choose if your VDAs must be non-domain-joined, Active Directory domain-joined, hybrid-joined, or Entra ID joined.

- Non-domain joined: VDAs in the catalog are not joined to an Active Directory domain.
- Active Directory: VDAs are joined to an Active Directory domain. A network connection is required for domain-joined VDAs. If selecting Active Directory, you must also input the **Fully qualified domain name (FQDN)**, **Organizational Unit (optional)**, **Service account name** (used for adding newly created VDAs to the domain), and a **Password** for the service account.
- Service Account: VDAs are joined to an Active Directory domain. You can create or select an existing Service Account to add newly created VDAs to the domain.
  - You can add or modify a Service Account in existing machine catalogs under the **Configuration** tab.
- Entra ID Hybrid-joined: VDAs are joined to Active Directory domain and Entra ID. A network connection is required for Hybrid domain-joined VDAs. If selecting Active Directory, you must also input the **Fully qualified domain name (FQDN)**, **Organizational Unit (optional)**, **Service account name** (used for adding newly created VDAs to the domain), and a **Password** for the service account.
- Entra ID: VDAs are joined to an Entra ID domain. An optional network connection can be used in combination with domain-joined VDAs to access internal resources. If selecting Entra ID, you must also create or select an existing Service Account and choose whether you want to enroll the machines in Microsoft Intune for device management capabilities.

e) **Specify the machine naming scheme**: Specify a naming scheme for the newly created machines. Use from one to four wildcards (hash marks) to indicate where sequential numbers or letters appear in the name. If you do not specify a naming scheme, the machines use the default naming scheme: DAS%%%%%-**-### where % is a random alphanumeric character matching the resource location prefix, * is a random alphanumeric character, and # is a sequential digit.

Rules:

- The naming scheme must contain at least one wildcard, but not more than four wildcards. All the wildcards must be together.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- The entire name, including wildcards, must be between 2 and 15 characters.
- A name cannot include blanks (spaces), slashes, backslashes, colons, asterisks, angle brackets, pipes, commas, tildes, exclamation points, at signs, dollar signs, percent signs, carets, parentheses, braces, or underscores.
- A name cannot begin with a period.
- A name cannot contain only numbers.
- Do not use the following letters at the end of a name: '-GATEWAY', '-GW', and '-TAC'.
- Leave enough room for growth.

  For example, a naming scheme with 2 wildcards and 13 other characters (for example, MachineSales-##) uses the maximum number of characters (15).

  Once the catalog contains 99 machines, the next machine creation fails. The service tries to create a machine with three digits (100), but that would create a name with 16 characters. The maximum is 15.

  So, in this example, a shorter name (for example, PC-Sales-##) allows scaling beyond 99 machines. Note: MCS adds an additional wildcard if all available spaces are taken and the machine name has not hit the character limit.

Wildcard (#) type: Indicate whether wildcards must be numbers (0-9) or letters (A-Z).

5. Configure the **Resource location** for the catalog. When creating an additional catalog with the same network connection, region, and domain name as another catalog, the resource location is reused. Non-domain joined catalogs in Citrix DaaS Flex have a resource location automatically created for them.

   a) **Resource location name**: Choose the resource location where your machines will reside.

   b) **Connectivity types**: Choose how endpoints connect to VDAs.

   - **Gateway service**: Uses a Citrix-managed Gateway for connectivity to virtual apps and desktops. HDX connections between clients and VDAs are proxied through the Gateway service.
   - **NetScaler Gateway**: Usa a customer-managed Gateway for external connectivity to apps and desktops. If you choose this option, you have to add the FQDN of your NetScaler Gateway virtual server.
   - **Direct**: Allow direct access to apps and desktops only for users on your corporate network. Users will not have external access.

6. Choose an **Image** for your catalog.

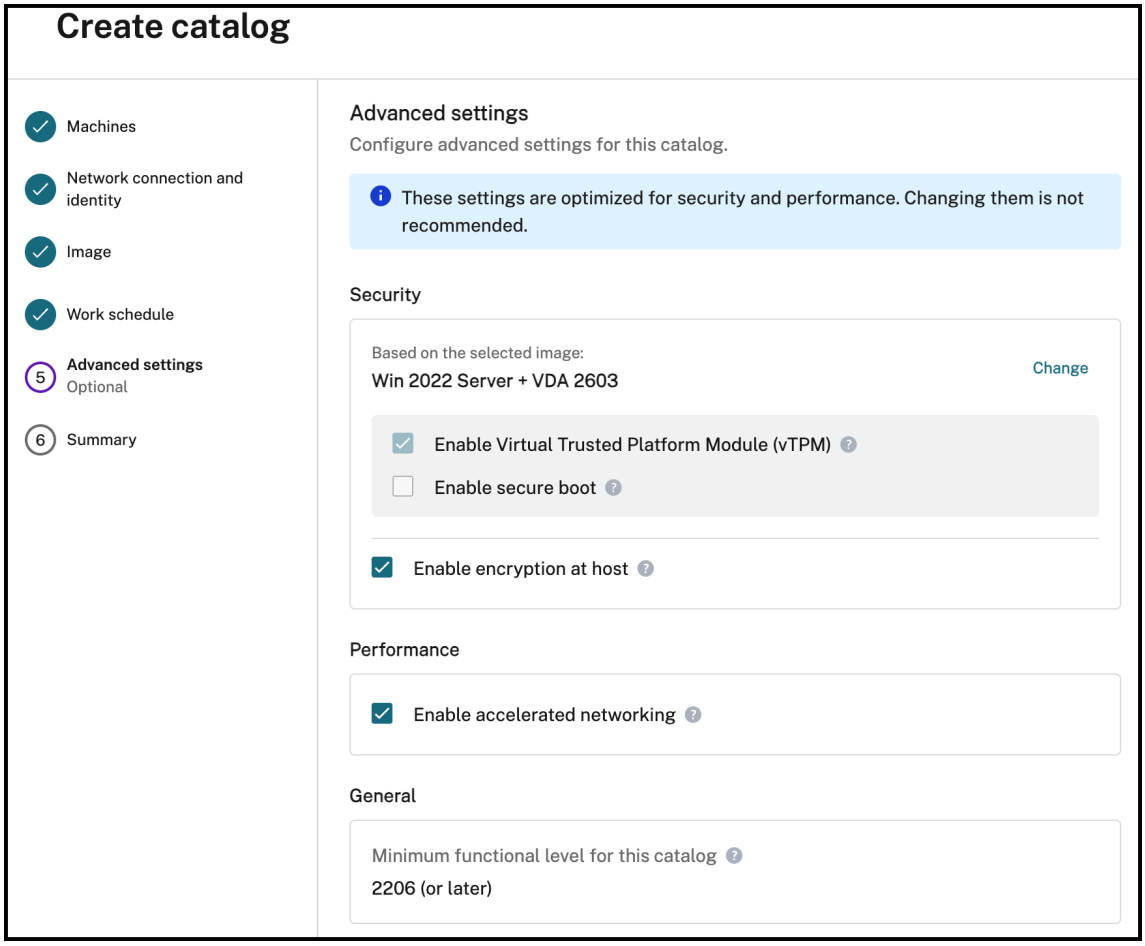
© 1997–2026 Citrix Systems, Inc. All rights reserved.

> **Note:**
>
> Only images compatible with your catalog (single-session vs multi-session, domain-joined vs non-domain-joined) are displayed in the dropdown.

7. Input the **Work schedule** of the users accessing the catalog. Citrix optimizes connectivity for the defined work schedule.

   a) **Time zone**: Choose the time zone of the users accessing the catalog.
   b) **Autoscale settings**: Consider using the Citrix-recommended default timeout and power policies to align with Citrix best practices. If customizations are required, select from the dropdown to define peak working hours and adjust timeouts and power policies.

8. Adjust **Advanced settings** as appropriate. For example, select **Enable Secure Boot** to ensure the best options are selected based on the image used.



9. Add a name for your catalog in the **Name your catalog** input.
10. Review the **Summary** of your configurations and click **Create Catalog** to begin provisioning machines to the catalog.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

> **Notes:**
>
> - When you create the first catalog, the Flex service automatically creates and enables a NAT Gateway to provide the internet connectivity that Flex components require to complete deployment. You can disable the NAT Gateway from within the catalog settings.
> - When you disable the NAT Gateway, you must provide alternative internet connectivity for the Flex components that require it for deployment and normal operation.

Add users to a catalog

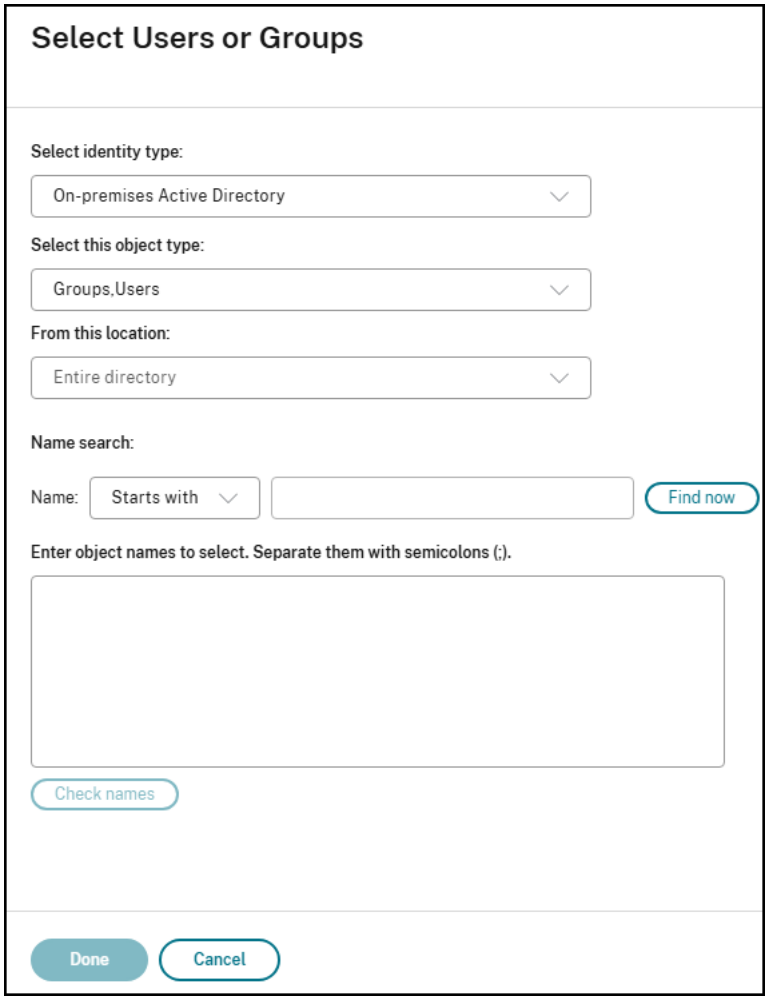
Once the catalog is provisioned, add users to the catalog to provide them access to the resources.

1. From the Citrix DaaS Flex dashboard, click **Give users access** if you haven't added any users to a catalog.



2. To add users to a catalog that already has users, click anywhere in the catalog's entry.
3. On the **Access** tab, click **Add Users**.
4. Select a directory and users or user groups.

© 1997–2026 Citrix Systems, Inc. All rights reserved.



5. When all users and groups have been added, click **Done**.

Remove users from the catalog

1. Click anywhere in the catalog's entry.
2. On the **Access** tab, click the trash icon next to the user or group you want to delete. This action removes the user from the catalog, not from the source.

Manage catalogs

October 5, 2026

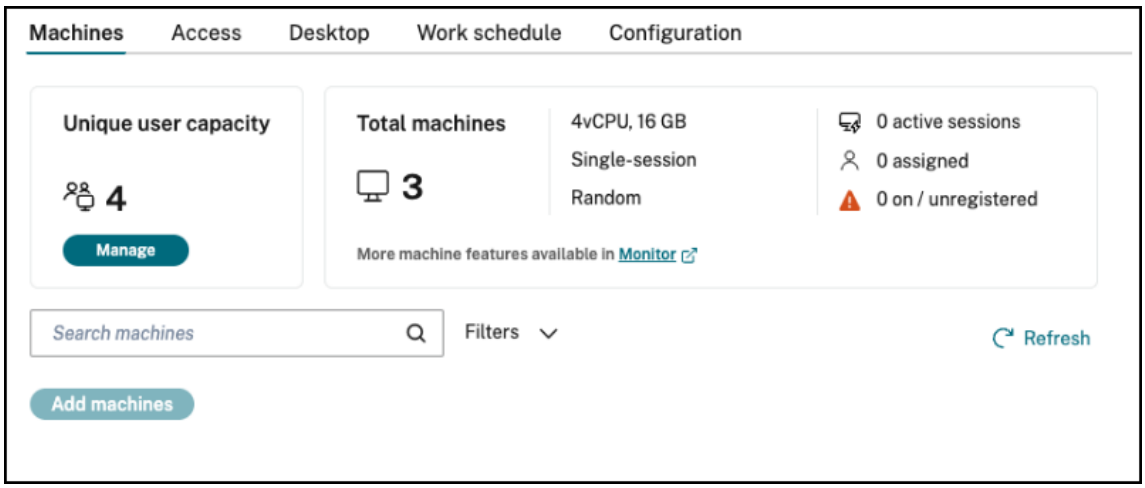
© 1997–2026 Citrix Systems, Inc. All rights reserved.

> **Note:**
>
> This article describes the tasks you can use to manage catalogs that were created in the Citrix DaaS Flex interface. For information about catalog management using the Web Studio management interface, see Manage machine catalogs.

Add machines to a catalog

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

1. From the **Quick Deploy > Microsoft Azure** dashboard, click a catalog.
2. On the **Machines** tab, click **Add Machines**.



3. Enter the number of users you want to add to the catalog.
4. If the VDAs in the catalog are Active Directory domain-joined, input a service account and password for adding the newly created VDAs to the domain.
5. Click **Add Machines**.

Manage user capacity in a catalog

1. From the Citrix DaaS Flex dashboard, select a catalog.
2. On the **Machines** tab, select **Manage** under the **Unique user capacity** section, then select **Change user capacity**:
    - **Increase capacity**: Increase the number of users that need to be added to that machine catalog. The corresponding number of machines are created to match the selected capacity.
        - Valid domain credentials or a Service Account is required.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

    - By default, the **Organizational Unit** entered during initial catalog creation will be displayed. You can either accept the default entry or modify the **Organizational Unit**, which will apply to all new machines created within the catalog.

- **Decrease capacity**: Decrease the number of users that have access to that machine catalog. The corresponding number of machines are removed to match the selected capacity. You cannot reduce the total number of users currently assigned to that machine catalog. Any machines chosen for deletion are presented to you prior to deletion for final acknowledgment.

> **Note:**
>
> - You are prompted with a message if your network connection does not have the available IP addresses required to provision the requested increased user capacity.
> - Machines with active user sessions cannot be removed. They must be placed into maintenance mode and drained of sessions before being deleted.
> - Estimated monthly credits are displayed based on the current machine catalog persona originally selected when the machine catalog was created.

Update a catalog with a new image

The behavior of updating the image of a catalog is determined by the catalog delivery model:

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

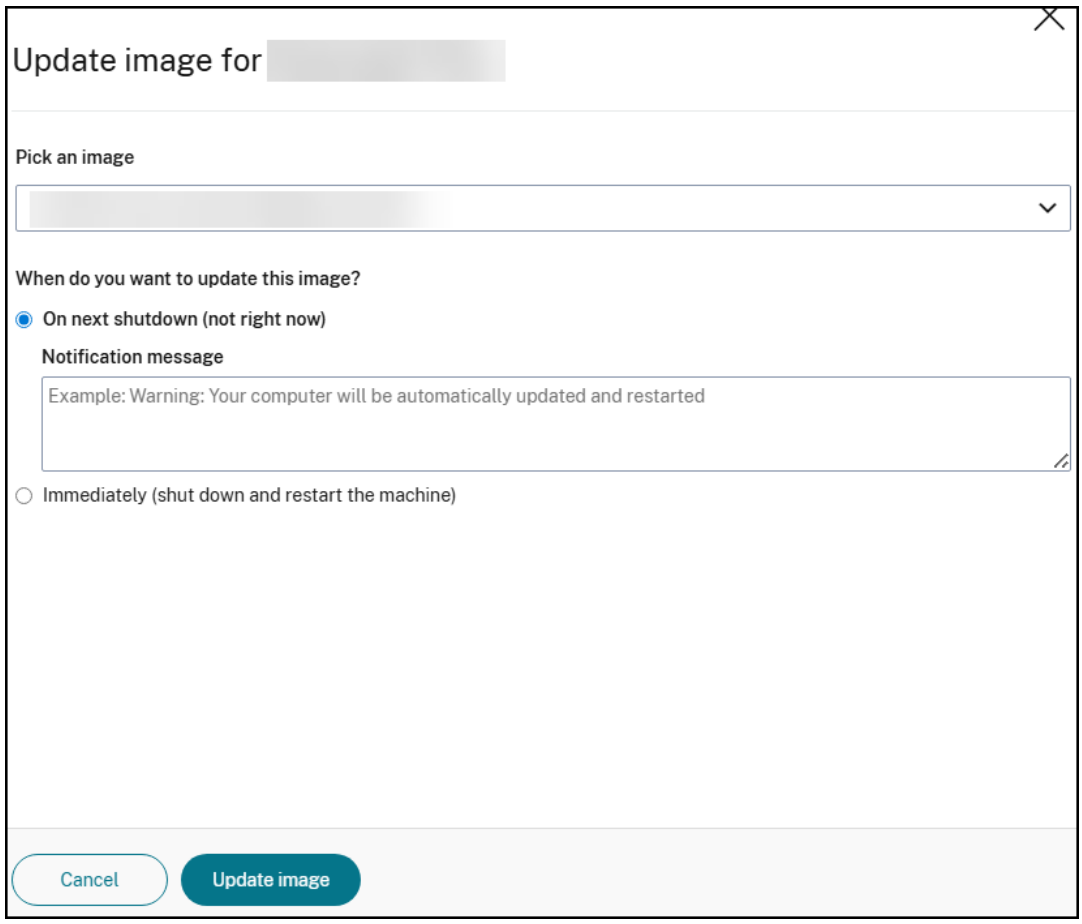
You can update a catalog containing machines with gen1 images with a gen2 image, if the catalog's machines support gen2. Similarly, you can update a catalog containing gen2 machines with a gen1 image, if the catalog's machines support gen1.

To update a catalog with a new image:

1. From the Citrix DaaS Flex dashboard, select a catalog.
2. On the **Desktop** tab, click **Update Image**.
3. Select an image.
4. For random or multi-session catalogs: Select when you want to update the image:

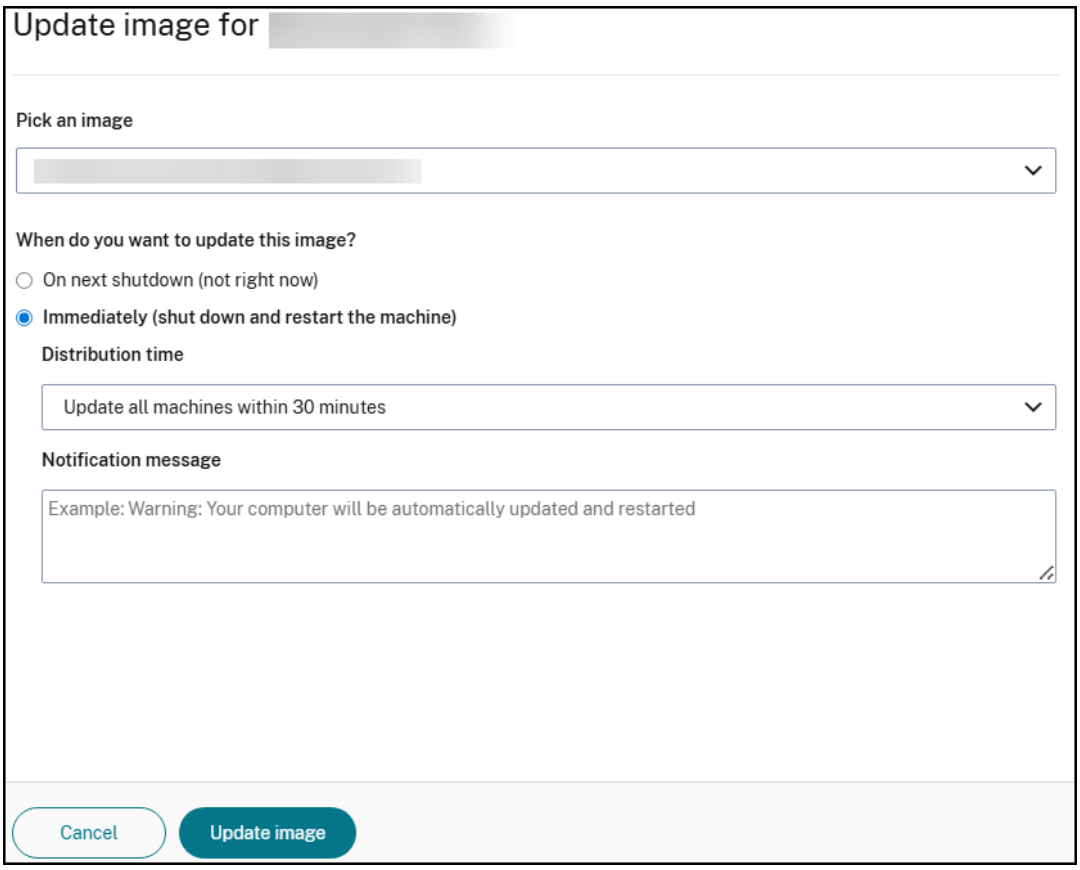
    - On next shutdown and enter notification message to the users

© 1997–2026 Citrix Systems, Inc. All rights reserved.



- Immediately and select the desired distribution time.

© 1997–2026 Citrix Systems, Inc. All rights reserved.



After Citrix DaaS Flex completes the initial image processing, users receive a warning to save their work and log off from their desktops.

5. Click **Update Image**.

Update a catalog identity type

You can convert an existing Active Directory (AD) only Citrix DaaS Flex catalog to Entra Hybrid Join (Hybrid Azure AD Join) without rebuilding it. The Machine Creation Services (MCS) provisioning engine runs the conversion as a scheduled maintenance cycle, so the catalog stays intact and its machines remain domain-joined while gaining Entra registration. The new identity type applies to newly provisioned VDAs immediately, and existing VMs are updated as they roll through their maintenance windows.

Prerequisites

Ensure that the catalog meets all of the following requirements before you begin the conversion:

- **Source catalog**: Citrix-managed (MCS), AD-joined only (not already Entra- or Azure AD–joined), single- or multi-session.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- **VDA version**: 2212 or later. The VDA must advertise the `AgentManagedHybridAzureAdJoin` capability.
- **Identity pool**: A non-shared pool that has an Active Directory service account configured.
- **Admin permissions**: Provisioning-scheme maintenance rights on the site, the same rights needed to schedule an image update.
- **Site feature**: `OrchMaintenanceCycle` must be enabled. It is on by default in Citrix DaaS.

You can start the conversion in either of the following ways:

Method 1 –Remote PowerShell SDK

Use the `New-ProvIdentityUpdate` cmdlet from the Citrix DaaS Remote PowerShell SDK. Before you run it, load the snap-ins with `asnp Citrix*` and authenticate with `Get-XDAuthentication`. For more information, see the New-ProvIdentityUpdate cmdlet reference.

```
New-ProvIdentityUpdate `
    -Operation MigrateActiveDirectoryToEntraHybridJoin `
    -ProvisioningSchemeName "<your-provisioning-scheme-name>" `
    -AllVMs `
    -MaintenanceCycleDescription "Convert AD catalog to Entra Hybrid
       Join" `
    -MaxDurationInMinutes 200
```

Key parameters:

- `-Operation MigrateActiveDirectoryToEntraHybridJoin`: Required. Specifies the conversion operation.
- `-ProvisioningSchemeName` or `-ProvisioningSchemeUid`: Identifies the catalog's provisioning scheme.
- `-AllVMs`: Applies the conversion to every VM in the scheme. To target specific machines instead, use `-VMName`.
- `-ScheduledStartTimeInUTC`: Optional. Sets a UTC start time. Omit it to start immediately.
- `-OU`: Optional. Specifies the AD OU for new computer accounts after conversion. Omit it to keep the existing OU.

Method 2 –Citrix DaaS REST API

The same conversion is available through the Citrix DaaS (Orchestration) REST API. Authenticate with a CWSAuth bearer token and pass your customer ID in the request headers. For more information, see ScheduleProvisioningSchemeIdentityUpdate.

Send a POST request to the following endpoint:

© 1997–2026 Citrix Systems, Inc. All rights reserved.

```
POST /{
 customerId }
 /{
 siteId }
 /provisioningSchemes/{
 nameOrId }
 /$scheduleIdentityUpdate
```

Include at least the following fields in the request body:

```
{

    "Operation": "MigrateActiveDirectoryToEntraHybridJoin",
    "Description": "Convert AD catalog to Entra Hybrid Join"
 }
```

The response returns a maintenance-cycle task ID. Poll the Tasks endpoint to track the task as it moves through the `Scheduled`, `InProgress`, and `Successful` or `PartiallyCompleted` states.

What changes after conversion

- The catalog's identity type changes from AD-joined to Entra Hybrid–joined. No machines are deleted or recreated.
- Newly provisioned VDAs come up as Entra Hybrid–joined right away.
- Existing VMs gain Entra registration as they cycle through their maintenance windows, so there is no single point at which every machine is converted.

> **Important:**
>
> The conversion cannot be reversed through the API. VDAs that have not yet cycled through a maintenance window remain AD-only until they do. To monitor per-machine status, use the Sub-Jobs endpoint (REST API) or the `Get-ProvTask` cmdlet (PowerShell SDK).

Manage machines in a catalog

1. From the Citrix DaaS Flex dashboard, select a catalog.
2. On the **Machines** tab, find the machine you want to manage. In the ellipsis menu for that machine, select the desired action:
    - **Restart**: Restart the selected machine.
    - **Start**: Start the selected machine. This action is available only if the machine is powered off.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- **Shutdown**: Shut down the selected machine. This action is available only if the machine is powered on.
- **Turn maintenance mode on or off**: Turn maintenance mode on or off for the selected machine.

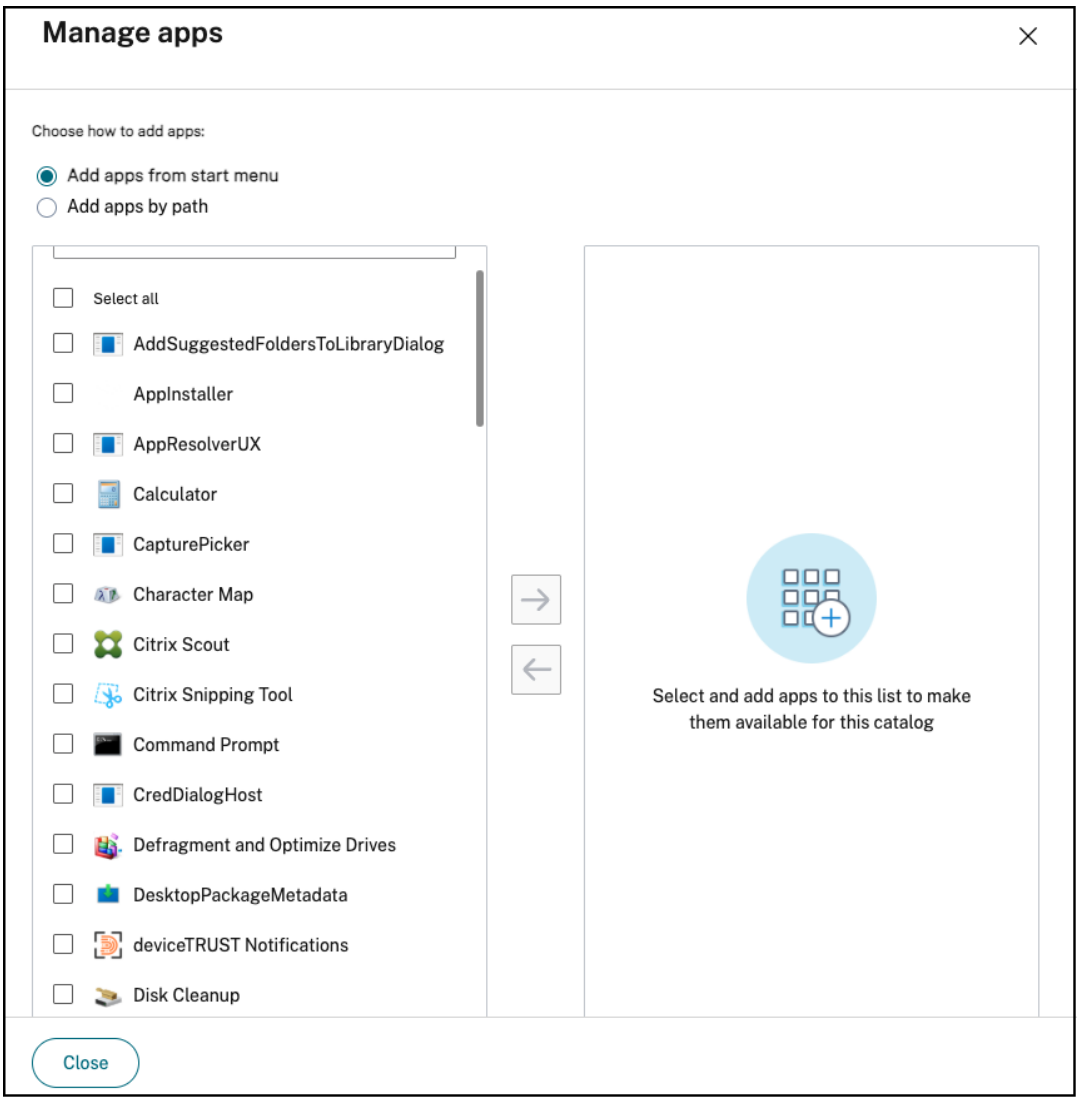
  By default, maintenance mode is turned off for a machine. Turning on maintenance mode for a machine prevents new connections from being made to that machine. Users can connect to existing sessions on that machine, but they cannot start new sessions. You might place a machine in maintenance mode before applying patches, or for troubleshooting.
- **Delete and adjust unique user capacity**: Delete the selected machines. This action is available only when the machine's session count is zero. Confirm the deletion by acknowledging the message boxes and entering your domain credentials, when required.

  When a machine is deleted, all data on the machine is removed. You cannot delete a machine when it is the last machine in the catalog.
- **Force restart**: Force a restart of the selected machine. Select this action only if a Restart action for the machine failed.

Add apps to a catalog

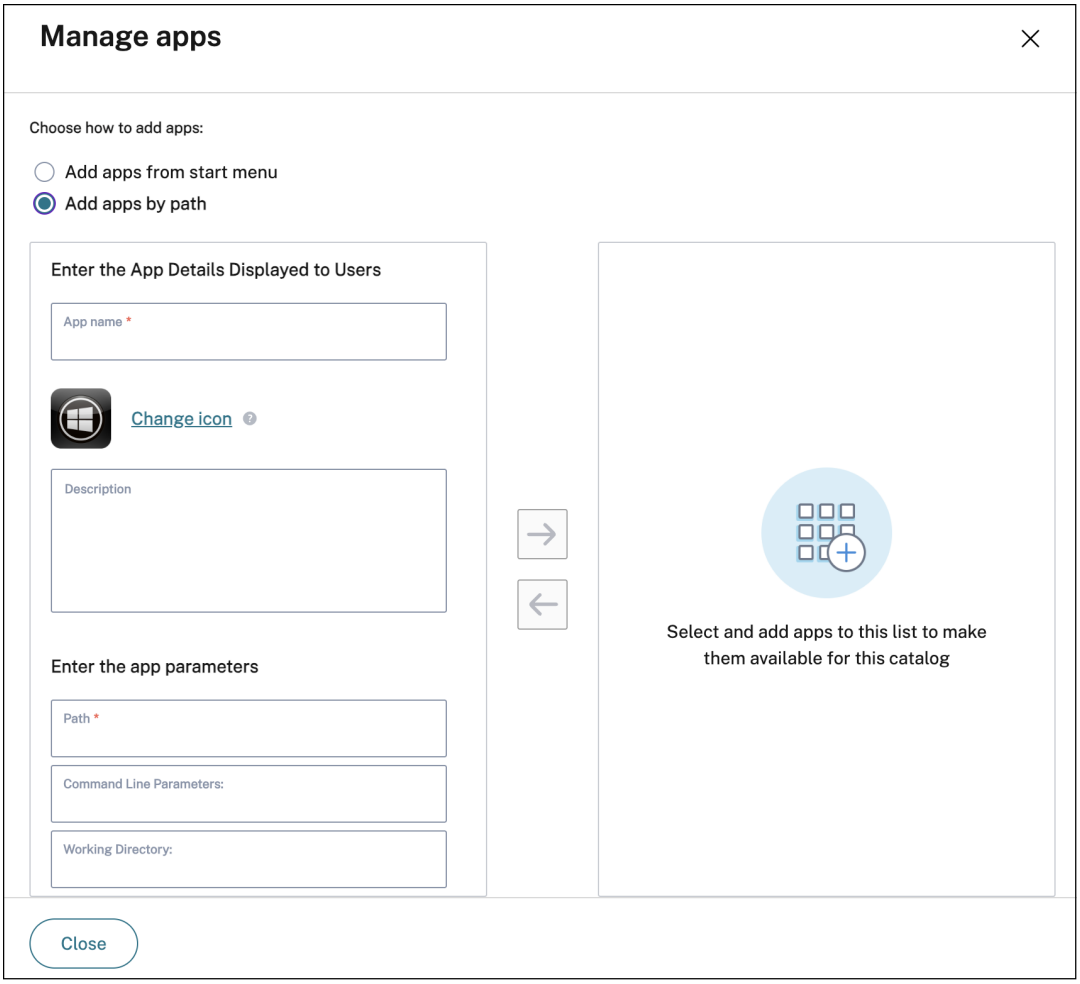
1. From the Citrix DaaS Flex dashboard, select a catalog.
2. On the **Desktop and apps** tab, click **Manage apps**.
3. Select how you are adding apps:
   - Add apps from Start Menu

© 1997–2026 Citrix Systems, Inc. All rights reserved.



- Add apps by path

© 1997–2026 Citrix Systems, Inc. All rights reserved.



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 in the right column are available in the Workspace or StoreFront portal for users assigned to the catalog.
     - 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.
   - **By path:**
     a) Enter the name for the app. This is the name users see in the Citrix Workspace or StoreFront portal.
     b) 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.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

c) Enter a description of the application (optional).
d) Enter the path to the app. Optionally, add command line parameters and the working directory. For details about command line parameters, see Pass parameters to published applications.

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

Edit an app in a catalog

1. From the **Quick Deploy > Microsoft Azure** dashboard, select a catalog.
2. On the **Desktop and apps** tab, click the row containing the app you want to edit.
3. Click the pencil icon.
4. Type changes in any of the following fields:

   - **Name**: The name of the application 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

© 1997–2026 Citrix Systems, Inc. All rights reserved.

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

> **Note:**
>
> Removing an app from a catalog does not remove it from the machines. It just removes it from users’ Citrix Workspace or StoreFront portal.

1. From the Citrix DaaS Flex dashboard, select a catalog.
2. On the **Desktop and apps** tab, click the trash icon next to the apps you want to remove.

Delete a catalog

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

1. Select a catalog.
2. On the **Machines** tab, click **Delete Catalog** on the lower portion of the window.
3. Confirm the deletion by selecting the acknowledgment check boxes and then clicking the confirmation button.

VDA snapshot and restore

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

You can configure daily and weekly snapshot schedules for all the machines in a catalog. These snapshots are called automatic snapshots. A snapshot is taken of each machine in the catalog. There are no default snapshot schedules.

You can take a manual snapshot of a single VM in a catalog on demand. You can create a manual snapshot of a machine even if the catalog it belongs to has scheduled snapshots. Scheduled snapshots can only be configured at the catalog level, not on individual machines.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

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

Snapshot schedules

Snapshot schedules apply to all machines in a catalog. Snapshot schedules are not configured by default.

To manage snapshot schedules:

1. From the Citrix DaaS Flex dashboard, select a catalog.
2. On the **Configuration** tab, click **Schedule Snapshots**.
3. On the **Schedule Snapshots** page, configure schedules for weekly or daily automatic snapshots, or both:
   - To add or change weekly snapshots, move the slider for **Weekly automatic snapshots** until a check mark appears. Select the day of the week and the start time.
   - To add or change daily snapshots, move the slider for **Daily automatic snapshots** until a check mark appears. Select the start time.
   - To remove weekly snapshots, move the slider for **Weekly automatic snapshots** until an **X** appears.
   - To remove daily snapshots, move the slider for **Daily automatic snapshots** until an **X** appears.
4. When you're done, click **Save**.

Manual snapshots

A manual snapshot is for a single machine in a catalog.

1. From the **Quick Deploy > Microsoft Azure** dashboard, select a catalog.
2. On the **Machines** tab, find the machine you want to take a snapshot of. Select **Snapshots** in the ellipsis menu for that machine.
3. On the **Snapshots for [VDA-name]** page, click **Create Manual Snapshot**.
4. Provide a name for the snapshot. Choose a name you can easily identify later.
5. Confirm your request.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

View and manage snapshots

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

    > **Note:**
    >
    > When you delete a catalog, all snapshots are destroyed.

Restore

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

1. From the Citrix DaaS Flex dashboard, select a catalog.
2. In the **Machines** tab, find the machine you want to take a snapshot of. Select **Snapshots** in the ellipsis menu for that machine.
3. On the **Snapshots for [VDA-name]** page, select the check box of the snapshot you want to use.
4. Click **Restore** in the table header.
5. Confirm the request.

The **Status** column on the **Machines** tab indicates the progress and outcome of the restore operation. If a machine fails to restore a snapshot, try again.

Monitor

May 11, 2026

© 1997–2026 Citrix Systems, Inc. All rights reserved.

From the Monitor dashboard, you can view desktop usage, sessions, and machines in your Citrix DaaS Flex 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.
2. Open the DaaS console.
3. Click the **Monitor** tab.

Citrix provides the same monitoring capabilities for Citrix DaaS Flex VDAs as Citrix DaaS VDAs. To learn more about monitoring VDAs, see Monitor.

> **Note:**
>
> Monitor capabilities around Cost Optimization, Right-sizing, AutoScale might not be available for Citrix DaaS Flex.

Delegated administration

October 13, 2026

A new built-in Quick Deploy Administrator role for enabling organizations to grant specific permissions to Flex administrators without requiring them to have full administrative access across the entire Citrix Cloud platform, thereby enhancing security and operational efficiency.

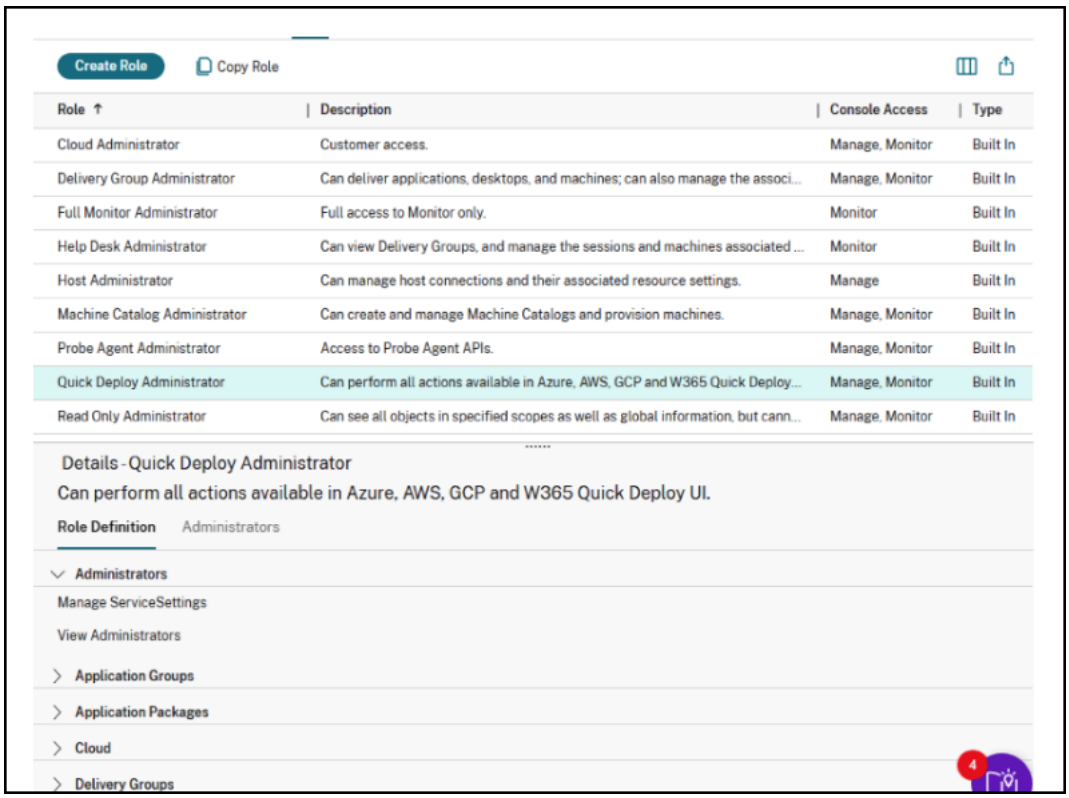
The benefits for Citrix Cloud Full Administrators are:

- Ability to securely delegate DaaS Flex-specific tasks to other team members.
- Improved organizational security and compliance.

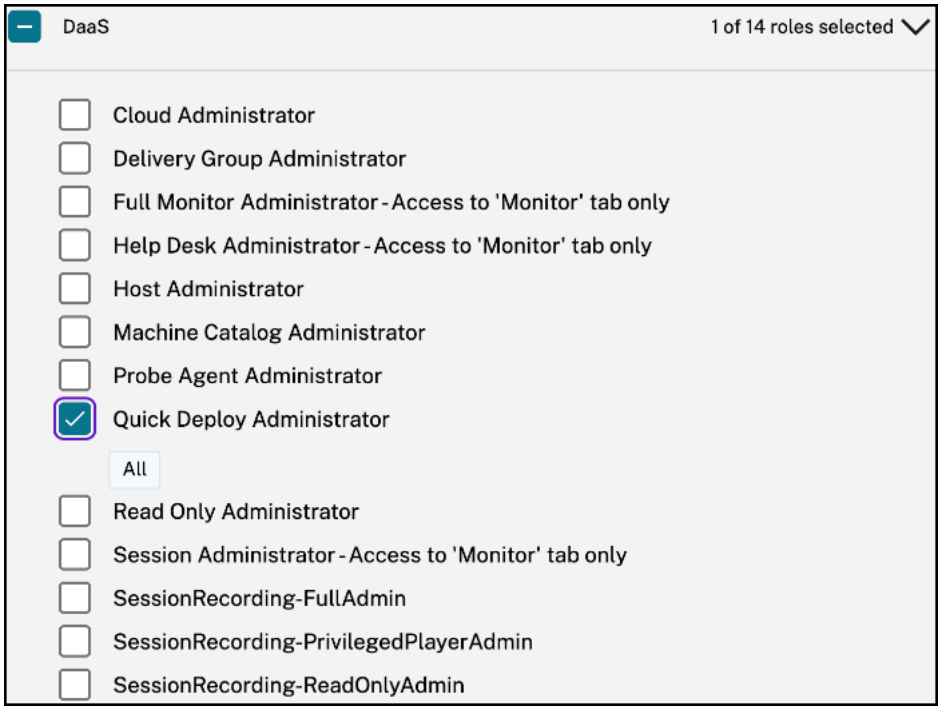
The benefits for designated **Flex Admins** are:

- Gain the necessary administrative control over DaaS Flex-related operations (for example, provisioning, monitoring, reporting) without being overwhelmed by unrelated permissions.
- Empowerment to manage their specific area effectively.

© 1997–2026 Citrix Systems, Inc. All rights reserved.



The new Quick Deploy Administrator role is accessible through Identity and access management.



Permission differences between full DaaS Cloud Administrator and Quick Deploy Administrator:

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Node	Cloud Admin Access	Quick Deploy Admin Access
StoreFronts	Yes	Read-only
Administrators	Yes	Read-only
Cost Management	Yes	No
Director/Monitor	Yes	No
SecureBrowser	Yes	No
Advisor	Yes	No
Download	Yes	Yes
Backup and restore	Yes	No
Quick Deploy	Yes	Yes
Home	Yes	Yes
Search	Yes	Yes
Application Groups	Yes	Yes
Application Packages	Yes	Yes
Delivery Group	Yes	Yes
Entitlement Policy Rules	Yes	Yes
Hosting	Yes	Yes
Images	Yes	Yes
Logging	Yes	Yes
Machine Catalogs	Yes	Yes
Policies	Yes	Yes
Service Accounts	Yes	Yes
Settings	Yes	Yes
UPM	Yes	Yes
Zone	Yes	Yes

Custom role and granular permissions in Quick Deploy

In a custom role of Quick Deploy for Azure, the granular permissions appear under the **Quick Deploy—Microsoft Azure** group. The group contains five permission categories. For each category, choose **No Access**, **Read Only**, or **Manage**. When you choose **Manage**, you can then select the individual

© 1997–2026 Citrix Systems, Inc. All rights reserved.

actions to allow.

Category	Read Only allows	Manage actions
Catalogs	View Quick Deploy catalogs	Create catalogs, Edit catalogs, Delete catalogs, Troubleshoot catalogs
Images	View Quick Deploy images	Build images, Import images, Edit images, Delete images
Network connections	View Quick Deploy network connections	Create network connections, Edit network connections, Delete network connections, Troubleshoot network connections
Subscriptions	View Quick Deploy subscriptions	Link subscriptions, Edit subscriptions, Rotate subscription credentials, Delete subscriptions
Troubleshoot and support	View Quick Deploy bastions and RDP access	Create bastions and RDP access, Edit bastions and RDP access, Delete bastions and RDP access

> **Note:**
>
> Read access is inclusive. Granting a broader permission automatically includes the read access it depends on, so you do not need to grant every read individually. For example, the ability to view catalogs also grants read access to the related images, network connections, and subscriptions, and every Manage action includes its own read access (for example, Edit catalogs includes View catalogs).

How to create a read-only Quick Deploy administrator

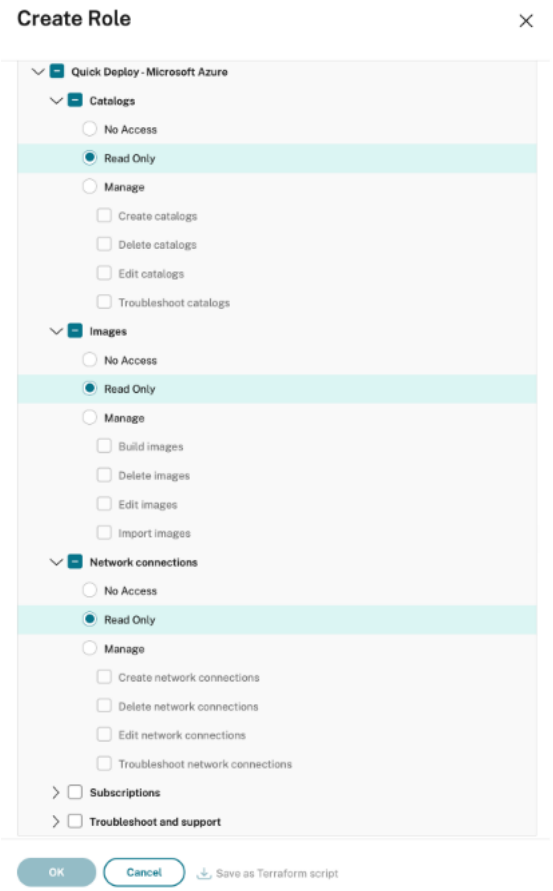
For a read-only reviewer across both standard DaaS Studio console and Quick Deploy, you can assign the built-in **Read-only Administrator** role, which already includes Quick Deploy read access.

In some situations, your company may have the policy to limit administrators to review Quick Deploy resources and settings only. Follow the steps below to create a custom dedicated Quick Deploy read-only role:

1. Sign in to Citrix Cloud and open Web Studio.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

2. Select **Administrators**, and then select the **Roles** tab.
3. Select **Create Role**.
4. Enter a **Name** (for example, XYZ Company Read-only Quick Deploy Admin) and a **Description** for the role.
5. Under **Console Access**, select **Manage**.
6. Under **Permissions**, expand **Quick Deploy** —**Microsoft Azure**.
7. Expand and set each subcategory —Catalogs, Images, Network connections, Subscriptions, and Troubleshoot and support —to **Read Only**.
8. Select **OK** to save the role.



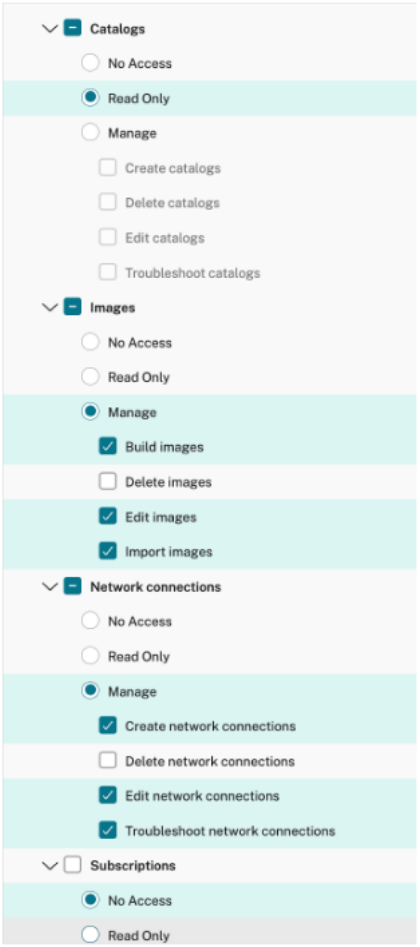
> **Tip:**
>
> Select **Save as Terraform script** in the role wizard to capture the role as infrastructure-as-code.

Create a Quick Deploy custom role with granular permissions

Use a custom role to grant a precise subset of permissions. The following example creates an image-and-network operator role that can manage images and network connections, view catalogs, and has no access to subscriptions.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

1. In Web Studio, select **Administrators** > **Roles**, and then select **Create Role**.
2. Enter a **Name** and a **Description** for the role.
3. Under **Console Access**, select **Manage**.
4. Under **Permissions**, expand **Quick Deploy** —**Microsoft Azure**, and then configure each subcategory:
   - **Catalogs**: select **Read Only**.
   - **Images**: select **Manage**, and then select the actions to allow (for example, Build images, Import images, and Edit images).
   - **Network connections**: select **Manage**, and then select the actions to allow (for example, Create network connections, Edit network connections, and Troubleshoot network connections).
   - **Subscriptions**: select **No Access**.
   - **Troubleshoot and support**: select **Read Only** or **Manage**, as required.
5. Select **OK** to save the role.



© 1997–2026 Citrix Systems, Inc. All rights reserved.

> **Note:**
>
> The individual action check boxes for a subcategory become available only after you select **Manage** for that subcategory.

To review or change an existing role:

1. Select **Administrators** > **Roles**.
2. Select the role. Its Quick Deploy permissions appear on the **Role Definition** tab in the lower panel.
3. Select **Edit Role** to change the permissions, or **Copy Role** to base a new role on it.

Assign a custom Quick Deploy role to an administrator

To assign a Quick Deploy role to an administrator:

1. In the Citrix Cloud console, navigate to **Identity and access management** > **Administrators**.
2. Add an administrator, or select an existing administrator and select **Edit access**.
3. Select the **Custom access** radio button, and then expand the **DaaS** section.
4. Assign the role you created, paired with the **All** scope.
5. Save your changes.

Review the Quick Deploy delegated administrator experience

When a delegated administrator signs in, the console reflects their permissions:

- The navigation shows only the nodes they can use —typically Home, Quick Deploy, and Settings for personal preferences.
- Under **Quick Deploy** > **Microsoft Azure**, the Catalogs and dashboard menu (Images, Network connections, Cloud subscriptions, Troubleshooting, and General) reflects the subcategories the administrator holds.
- With read-only access, resources are visible, but change actions such as Create catalog, Edit, Delete, and Add machines are hidden or unavailable.
- Actions the administrator cannot perform do not appear. A button, tab, or menu item is shown only when the service accepts the corresponding request.

Functions reserved for full administrators

Some tenant-wide functions are not delegated through granular Quick Deploy permissions. They continue to require a Cloud Administrator or Quick Deploy Administrator, or, where noted, a full Citrix Cloud administrator:

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- User profiles (profile management, the dashboard panel, and the catalog profile-store step).
- User access and authentication (the panel and workspace authentication settings).
- Consumption (consumption status, panel, and alerts).
- Global site settings (editing; other administrators see these settings as read-only).
- Cancel subscription —requires a full Citrix Cloud administrator.

Limitations

- Object scopes are not supported for Quick Deploy in this release. Always pair Quick Deploy custom roles with the **All** scope.
- Granular Quick Deploy permissions are available only to DaaS Flex for Azure customers.

Microsoft Entra ID

June 23, 2026

Support for Microsoft Entra ID and Intune allows Citrix DaaS Flex to extend identity, access, and device management capabilities, helping organizations improve security posture, support compliance requirements, and streamline the end-user experience. Combining this functionality with Microsoft Entra single sign-on provides users with a seamless experience.

Configure Microsoft Entra ID identity

Create an Entra ID App Registration

1. In your Azure portal, navigate to **Entra ID** > **App registration** > **New registration**.
2. Register a new application.

   > **Note:**
   >
   > The Azure administrator must have multifactor authentication configured.

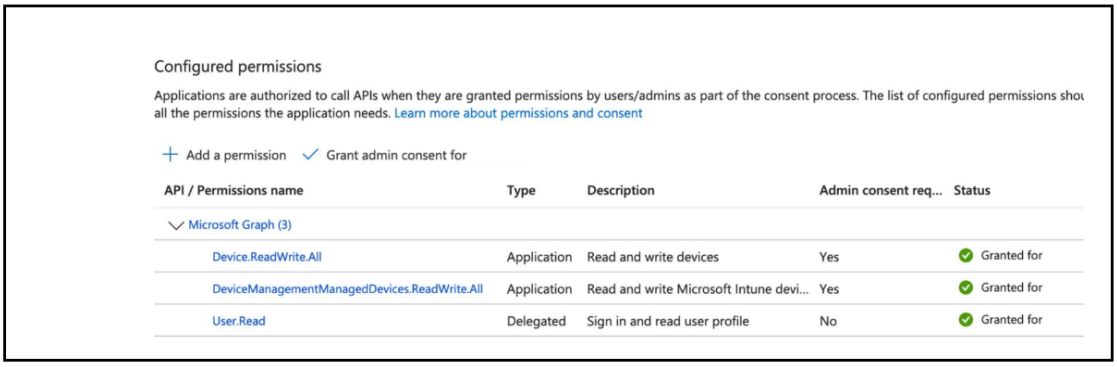
3. On the overview page, copy and save the following values:
   - Application (client) ID
   - Directory (tenant) ID
4. In the left sidebar, click **Certificates & Secrets** > **New client secret**.
5. Fill in the **Description** field and choose an expiration duration for the client secret.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

> **Note:**
>
> You will be prompted for this expiration date in a later step within the Citrix console.

6. Immediately copy the **Value** column. This is your client secret and is only shown once.
7. In the left sidebar, click **API permissions** > **Add a permission** > **Microsoft Graph** > **Application permissions**.
8. Search for and select the following permissions:
   - `Device.ReadWrite.All` —required for Entra ID registration
   - `DeviceManagementManagedDevices.ReadWrite.All` —required for Intune device enrollment
9. Click **Add permissions**.
10. On the **API permissions** page, click **Grant admin consent for <`tenant name`>**, then click **Yes** to confirm.

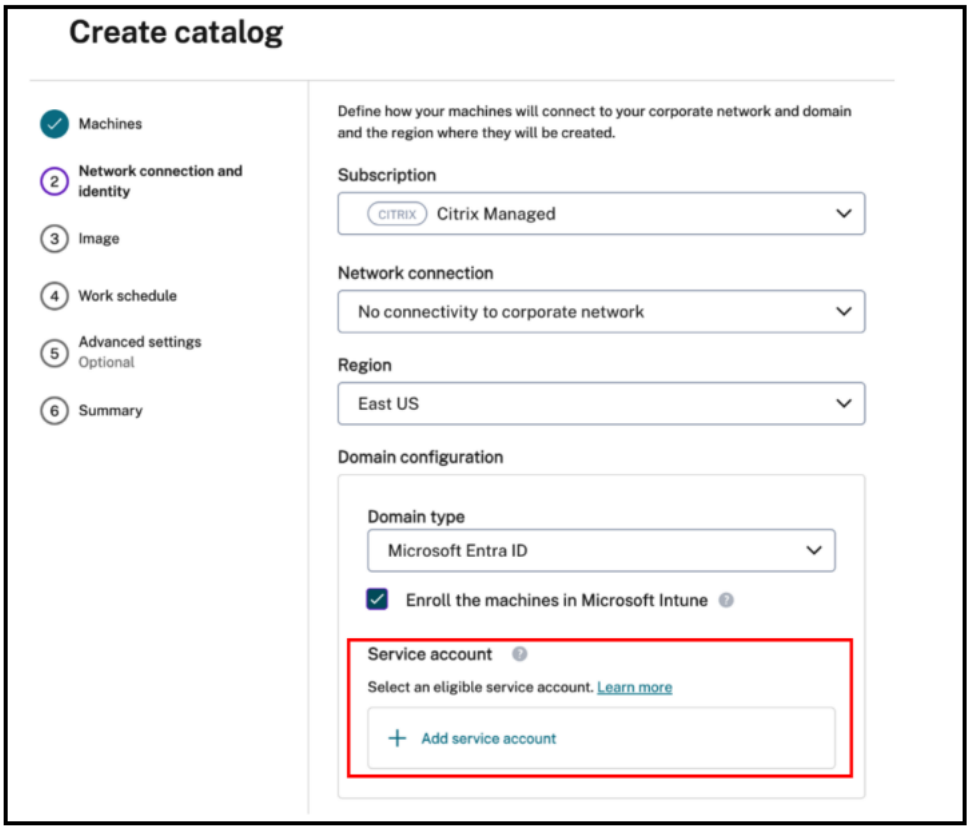
> **Note:**
>
> Verify that both permissions show a green checkmark under the **Status** column.



Create a Service Account

During the Create catalog workflow, a Microsoft Entra ID service account is required. For more information, see Azure AD service accounts.

© 1997–2026 Citrix Systems, Inc. All rights reserved.



Enable Entra ID Single Sign-On

Microsoft Entra ID Single Sign-On (SSO) allows users to authenticate once using their Entra ID credentials and gain seamless access to virtual applications and desktops without being prompted to sign in again. SSO is supported for session hosts that are Microsoft Entra joined or Microsoft Entra hybrid joined.

For more information on configuration, see Enable Entra ID SSO for virtual apps and desktops.

Troubleshoot

October 7, 2026

Introduction

Resource locations contain the machines that deliver desktops and apps. Those machines are created in catalogs, so the catalogs are considered part of the resource location. Each resource location also

© 1997–2026 Citrix Systems, Inc. All rights reserved.

contains Cloud Connectors. Cloud Connectors enable Citrix Cloud to communicate with the resource location. Citrix installs and updates the Cloud Connectors.

Optionally, you can initiate several Cloud Connector and resource location actions. See Resource locations

Citrix DaaS Flex has troubleshooting and supportability tools that can help resolve configuration and communication issues with VDAs. For example, creating a catalog might fail, or users might be unable to start their desktop or apps.

This troubleshooting includes gaining access to your Citrix DaaS Flex subscription through a bastion machine or direct RDP. After gaining access to the subscription, you can use Citrix supportability tools to locate and resolve issues.

For details, see:

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

Troubleshooting catalog using UI

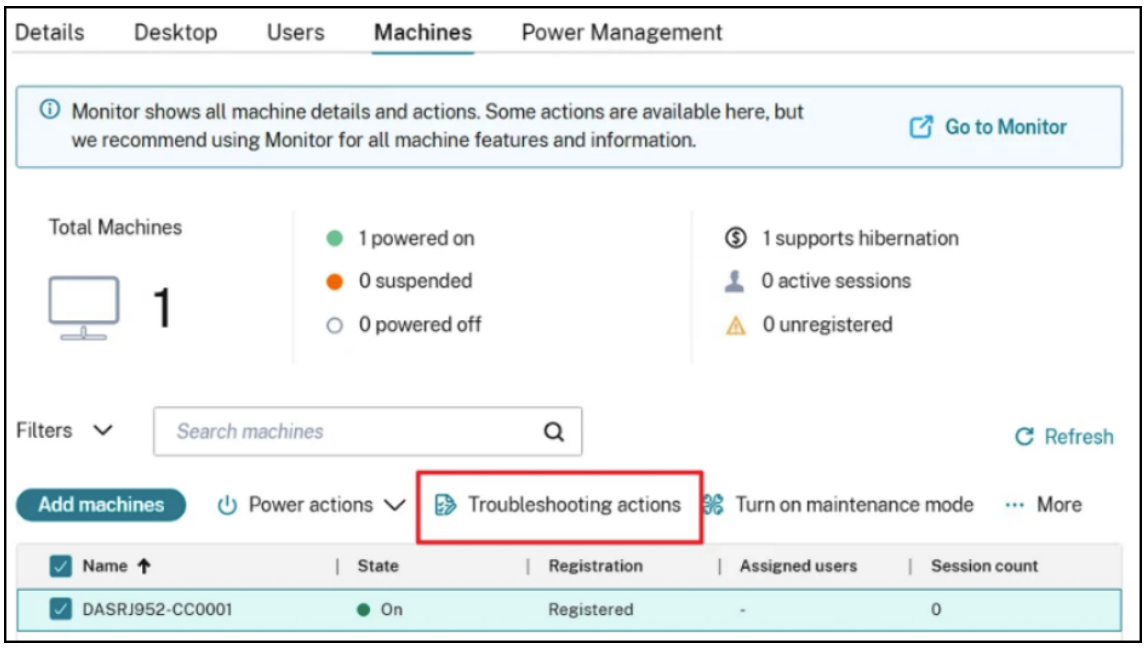
In the event the customer experiences problems with the catalog in Citrix DaaS Flex, the first option is to use the troubleshooting tool that enables customer administrators to diagnose and resolve issues in Flex catalogs directly from the **Quick Deploy** console.

> **Notes:**
>
> - This feature is currently available for Windows machines only.
> - To use this option the machines must be able to resolve *.blob.core.windows.net to upload the resultant logs.

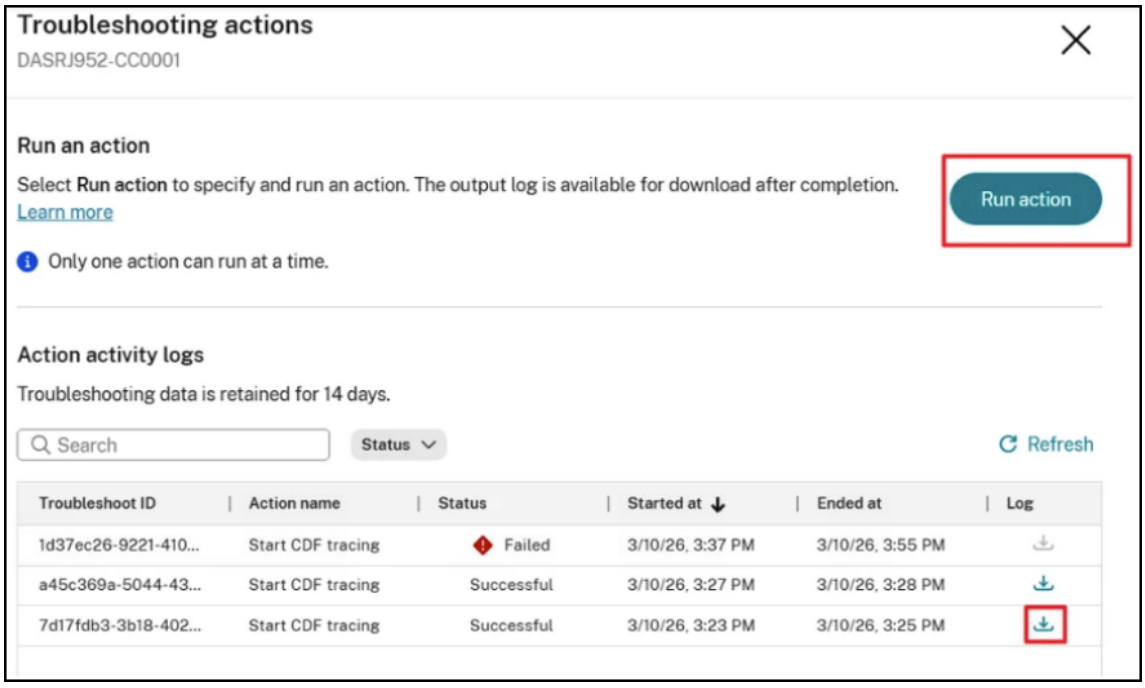
The feature provides machine level troubleshooting actions, secure access options, and execution history in a single, guided workflow.

1. Sign in to the Quick Deploy console.
2. Navigate to Microsoft Azure catalogs.
3. Select a Flex catalog that needs to troubleshoot, and select **Machine**s tab.
4. Select the relevant machine, and click on **Troubleshooting actions**.

© 1997–2026 Citrix Systems, Inc. All rights reserved.



5. Click **Run action** and specify the action.



After running an action, a new activity entry appears in the logs with **Running** status, which updates to **Successful** or **Failed** upon completion, then you can download the output log.

Troubleshooting and Support page

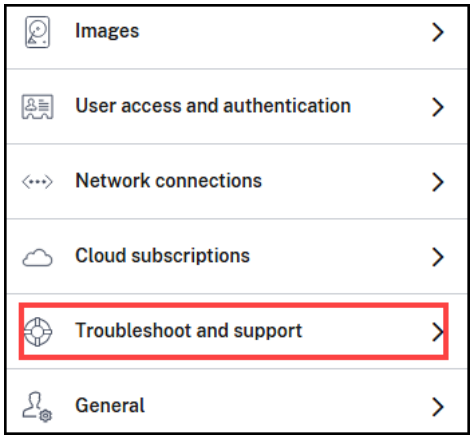
There are two additional options for troubleshooting:

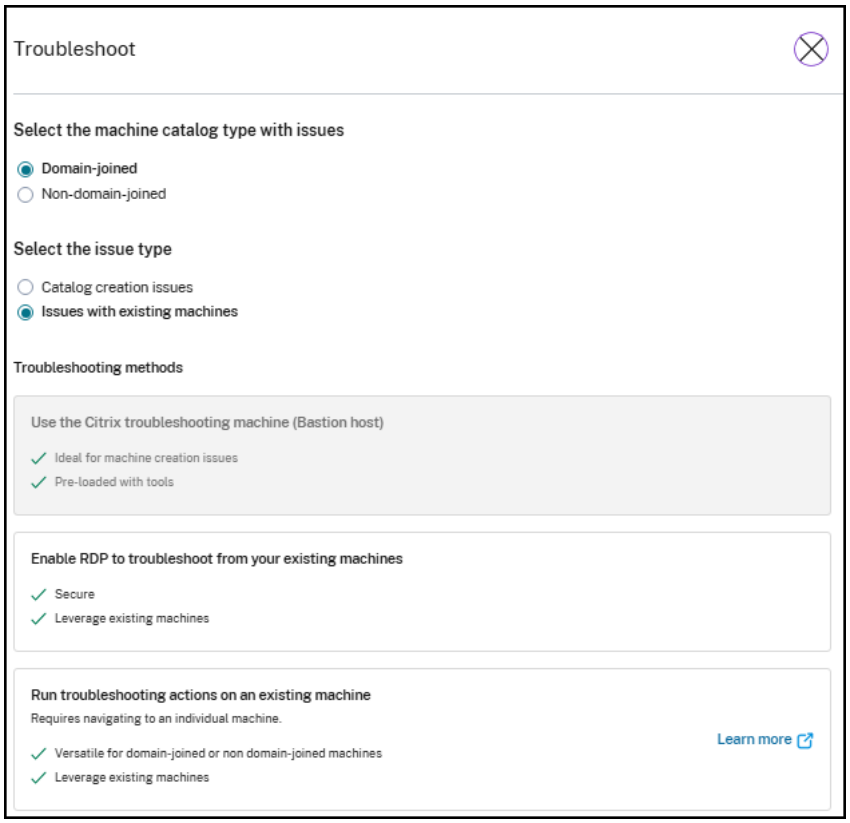
© 1997–2026 Citrix Systems, Inc. All rights reserved.

- Using bastions
- Enabling RDP access

Both options require the opening of the RDP port, 3389, to perform troubleshooting actions. You must consent to opening these ports prior to the port being opened. Citrix automates the opening and closing of the necessary ports to carry out troubleshooting operations and restricting the machines that can be accessed during these operations.

Navigate to **Troubleshoot and support > View troubleshooting options** to access the troubleshooting options page.





© 1997–2026 Citrix Systems, Inc. All rights reserved.

VDA troubleshooting using a bastion or direct RDP

> **Note:**
>
> These supportability features are valid only for domain-joined machines. If the machines in your catalogs are not domain joined, request troubleshooting help from Citrix Support.

Access methods

Two supportability access methods are provided:

- Access your resources through a bastion machine in the Citrix DaaS Flex 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 bastion machine is intended for short-term use. This method is intended for issues involving the creation of catalogs or image machines.

  To access a bastion machine:

  1. Create the bastion machine.
  2. Download an RDP file.
  3. RDP to the bastion machine.
  4. Connect from the bastion machine to the other Citrix machines in your subscription.

- Direct RDP access to the machines in the customer's dedicated Citrix DaaS Flex 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.

> **Note:**
>
> As an alternative to these two access methods, contact Citrix Support for assistance.

Bastion access

1. From the Citrix DaaS Flex dashboard, expand **Troubleshoot and Support**.
2. Click **View troubleshooting options**.
3. On the **Troubleshoot** page, select **Catalog creation issues**.
4. Select **Use the Citrix troubleshooting machine (Bastion host)** as the Troubleshooting method.
5. On the **Troubleshoot with Bastion Machine** page, select the catalog.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

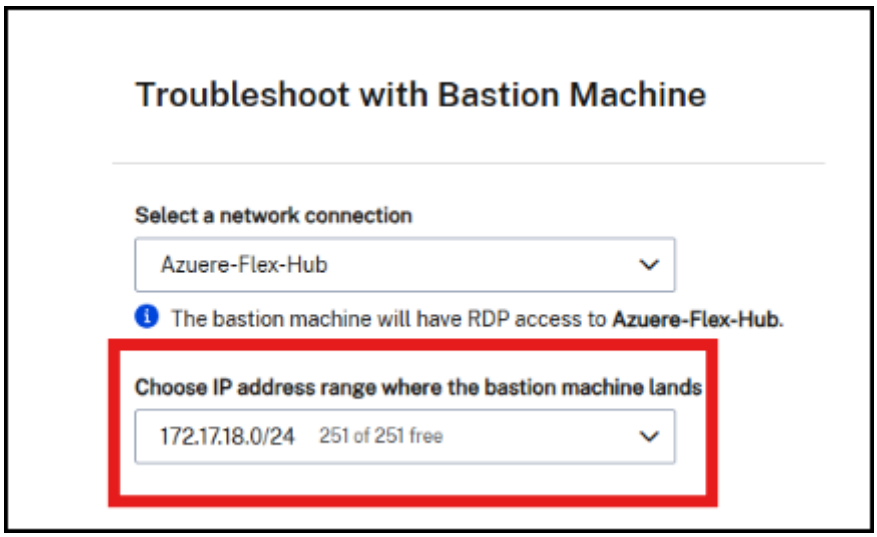
- If the machines in the selected catalog are not domain joined, you're instructed to contact Citrix Support.
- If a bastion machine has already been created with RDP access to the selected catalog's network connection, then select **Download RDP File**.

6. Type a username and password that you will use to log in when you RDP to the bastion machine. See Microsoft's Password requirements for more information. Do not use Unicode characters in the username.
7. The **Bastion access duration** is displayed. Citrix requires restricting Bastion access to a specific time-based duration. You can choose between 2, 4, and 8-hour durations. Once the time expires, any open Bastion sessions, firewall rules, and network routes will be closed.

   - The remaining time for your Bastion session will be displayed within the active Bastion troubleshooting configuration pane.

8. The **RDP access range** is displayed. Citrix requires restricting RDP access to a smaller range than permitted by the network connection. Select **Add IP ranges** and then enter the desired range (max /24). You can create up to 5 unique ranges.
9. Select an **IP address range** for the bastion machine. This controls which subnet the bastion's network interface is placed in, so that it can reach the machines you need to troubleshoot in a segmented network.

   The **IP address range** dropdown lists every CIDR block in the selected network connection's address space. Each entry shows its available capacity, for example "231 of 251 free". Choose the range that can reach the subnet you want to troubleshoot.



   Keep the following behaviors in mind:

   - **If you leave the field empty**: Citrix omits the placement preference, and Azure allocates

© 1997–2026 Citrix Systems, Inc. All rights reserved.

an address dynamically. This is the default behavior that applied before this option was available.

- **If the range shows no free addresses**: A range reporting 0 free addresses remains selectable but displays a warning. The count is advisory, because the address is allocated when the bastion is created. If allocation fails, an error naming the rejected CIDR block appears under the dropdown. Select a different range and try again.
- **If you change the network connection**: Citrix clears your IP address range selection and reloads the list for the new connection.
- **After the bastion is created**: The bastion details blade shows the **Bastion IP address range** and **Bastion private IP address**, confirming the range used and the exact address assigned.

10. Click **Create Bastion Machine**.

    - When the bastion machine is successfully created, the page title changes to **Bastion –connection**.
    - If the bastion machine creation fails, click **Delete** at the bottom of the failure notification page and try to create the bastion machine again.
    - Click **Edit** to change the RDP range restriction after the bastion machine is created. Enter the new value and then click the check mark to save the change.

11. Click **Download RDP File**.
12. Open the RDP file to RDP to the bastion, using the credentials you specified when creating the bastion.
13. 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. Bastion 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 Citrix DaaS Flex dashboard, expand **Troubleshoot and Support**.
2. Click **View troubleshooting options**.
3. On the **Troubleshoot** page, select **Issues with existing machines**.
4. Select **Enable RDP to troubleshoot from your existing machines** as the troubleshooting method.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

5. On the **Troubleshoot with RDP Access** page, select the catalog's network connection.
    - If RDP has already been enabled for the selected catalog's network connection, then connect to machines using your Active Directory administrator credentials. You can then collect logs and run diagnostics.
6. The **RDP access duration** is displayed. Citrix requires restricting RDP access to a specific time-based duration. You can choose between 2, 4, and 8-hour durations. Once the time expires, any open RDP sessions, firewall rules, and network routes will be closed.
    - The remaining time for your RDP session will be displayed within the active RDP troubleshooting configuration pane.
7. The **RDP access range** is displayed. Citrix requires restricting RDP access to a smaller range than permitted by the network connection. Select **Add IP ranges** and then enter the desired range. (max /24). You can create up to 5 unique ranges.
8. Click **Enable RDP Access**.
    - When RDP access is successfully enabled, the page title changes to **RDP Access –connection name**.
    - If RDP access is not successfully enabled, click **Retry Enabling RDP** at the bottom of the failure notification page.
9. Connect to machines using your Active Directory administrator credentials. You can then collect logs and run diagnostics.

Get help

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

Citrix DaaS Flex for AWS (Tech Preview)

July 24, 2026

Citrix DaaS Flex is the simplest, fastest way to deliver virtual apps and desktops to any device. Delivered through Citrix Cloud, this persona-based service streamlines your operations with cloud-based management, rapid provisioning, and fully managed capacity.

Citrix DaaS Flex includes:

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- Cloud-based management and provisioning of VDAs hosted in Citrix-managed cloud subscriptions.
- High-definition user experience across a broad range of devices.
- Simplified image lifecycle management using Citrix-prepared and customer-provided images.
- Integrated monitoring and operational visibility.
- Compatibility with existing Citrix DaaS architectures.

Citrix is now inviting selected customers to participate in the Tech Preview of DaaS Flex for AWS. Providing early access to evaluate its differentiated value and to showcase the technical and business benefits of this approach. For additional information sign into the Citrix DaaS Console and select the Resource Center (bottom right purple icon).

Important information and documents

June 17, 2026

- Trust Center Certifications
- Security, privacy, and compliance for products and services
- Citrix DaaS and Citrix DaaS Flex Due Diligence Package
- Cloud Software Group Services Security Exhibit
- Cloud Software Group Data Processing Addendum

Service Level Agreement

September 25, 2026

This Service Level Agreement (SLA) describes Citrix's commitment for the Citrix® Platform Flex offering and supersedes the service level terms described in the Citrix Cloud Service Level Agreement. This SLA is part of the Cloud Software Group end user agreement (EUA) for covered services ("Services").

Measure for Monthly Uptime

The following table describes the service and the measure of availability:

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Service	Measure of Availability
Citrix® DaaS Flex for Azure	Time users can access their app or desktop sessions through the Service.
Citrix DaaS	Time users can access their app or desktop sessions through the Service.
Citrix Secure Private Access™	Time users can access their SaaS or internal web app through the Service.
Citrix SecurSpaces Flex for Azure	Time users can access their workspaces through the Service.

> **Note:**
>
> - For DaaS and DaaS Flex, Service Continuity or Local Host Cache must be correctly configured and validated for the tenant to be eligible for the Service Level Agreement.
> - Citrix Gateway Service for HDX™ Proxy, Citrix Workspace™, License Activation Service (LAS) are component services. These components do not have independent SLAs or standalone uptime commitments and the Service Commitment and Remedies for these components are incorporated into and governed by the Citrix DaaS, DaaS Flex SLAs, or Citrix Secure Private Access when applicable.

Citrix's service commitment ("Service Commitment") is to maintain at least 99.9% monthly uptime ("Monthly Uptime") on the Service. Monthly Uptime is calculated by subtracting from 100% the percentage of minutes during a full month of the Service in which the Service instance was in the state of not Available as defined above. Monthly Uptime percentage measurements exclude downtime resulting from:

- Regularly scheduled maintenance windows.
- Customers' failure to follow configuration requirements for the Service as documented on Citrix Product documentation, or abusive behavior, or faulty input.
- Customer's use of a Service after Citrix® advised Customer to modify Customer's use of the Service, if Customer did not modify use.
- Caused by any component not managed by Citrix including, but not limited to, Customer's controlled physical and virtual machines, Customer installed and maintained operating systems, Customer installed and controlled software, networking equipment or other hardware; Customer defined and controlled security settings, group policies, and other configuration policies; public cloud provider failures, Internet Service Provider failures; or other Customer support factors external to Citrix's control.
- Customer's employees, agents, contractors, or vendors, or anyone gaining access with Customer's passwords or equipment or otherwise resulting from Customer's failure to follow appropriate security practices.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- Customer's attempts to perform operations that exceed Service entitlements.
- Service disruption due to Force Majeure, including, but not limited to, natural disasters, war or acts of terrorism, or government actions.
- Caused by the unavailability of the underlying Microsoft Azure platform including but not limited to the inability of the Azure platform to start, stop, restart, or resume a user's virtual machine.
- For DaaS Flex, if the VMs were hibernated or powered off, Citrix triggers resume or power on. The time the VMs were powered off or hibernated is not part of the SLA.

Service Commitment and Remedies

If Citrix fails to meet the Service Commitment, and the failure affects 50% or more of users entitled to use the Service for at least 3 out of any 5 consecutive months, the Customer's exclusive remedy is a Service Credit. The Service Credit equals 5% of the Citrix Platform Flex credits consumed for the applicable Service during the months in which Citrix failed to meet the Service Commitment, capped at the total Citrix Platform Flex credits purchased. Service Credits may only be applied toward the Customer's next Citrix Platform Flex renewal and expire if not used within that period. Only one Service Credit is issued per Service, with a maximum of a single 5% Citrix Platform Flex credit for the term.

To receive the above remedy, the customer must be in compliance with the EUA and the failure must be reported by the customer within thirty (30) days of the end of the last month of the consecutive five-month period for which a credit claim is to be made. For instructions to report possible violations of this SLA, see CTX237141.

The request must identify the Services, define the dates, times, and durations of Unavailability, along with supporting logs or records that corroborate the Unavailability, and identify the affected users and their locations, and any technical support requested or remediation implemented.

© 2025 Cloud Software Group, Inc. All rights reserved. This document is subject to U.S. and international copyright laws and treaties. No part of this document may be reproduced in any form without the written authorization of Cloud Software Group, Inc. This and other products of Cloud Software Group may be covered by registered patents. For details, please refer to the Virtual Patent Marking document located at https://www.cloud.com/legal. Citrix, the Citrix logo, NetScaler, and the NetScaler logo and other marks appearing herein are either registered trademarks or trademarks of Cloud Software Group, Inc. and/or its subsidiaries in the United States and/or other countries. Other marks are the property of their respective owner(s) and are mentioned for identification purposes only. Please refer to Cloud SG's Trademark Guidelines and Third Party Trademark Notices (https://www.cloud.com/legal) for more information.